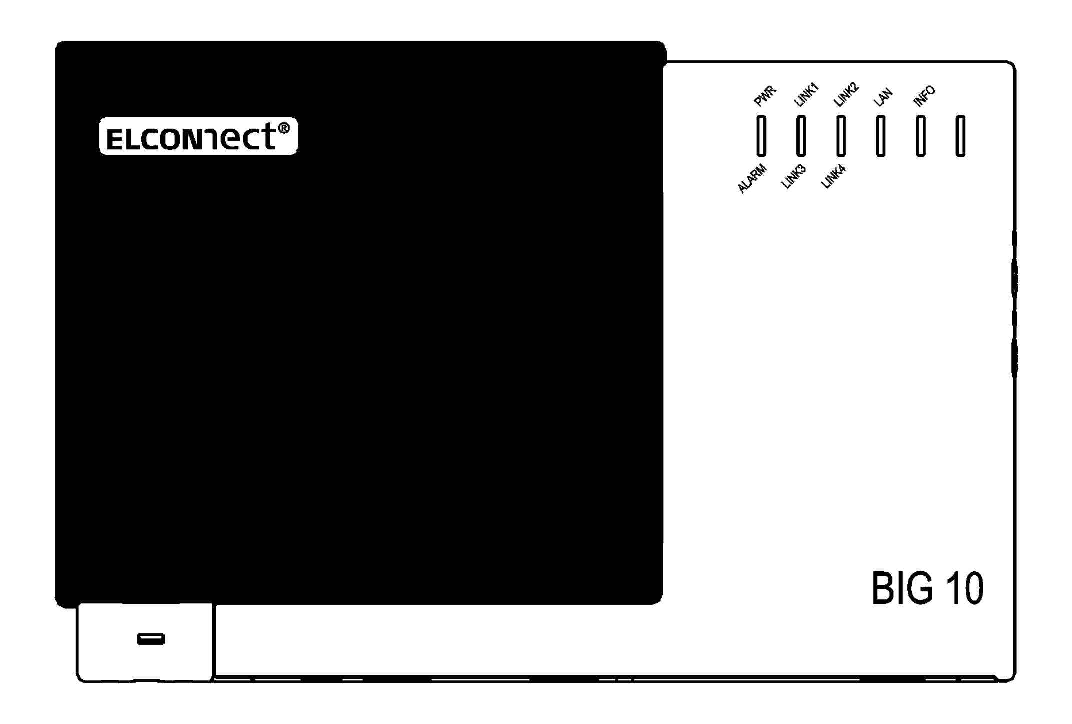


ELCONnect® next BIG 10 Router

Business IP Gateway



Bedienungsanleitung

Operating Instructions

 Art.-Nr. 102769-1

Sicherheitshinweise

- Bitte lesen Sie die Warnhinweise, Sicherheitsbestimmungen sowie die Bedienungsanleitung gewissenhaft durch, bevor Sie mit der Installation des BIG 10 beginnen. Nur so können Sie das Gerät in seinem vollen Funktionsumfang nutzen und Schäden durch unsachgemäßen Gebrauch vermeiden (Feuer, Elektroschocks, Verletzungen usw.). Bewahren Sie die Bedienungsanleitung sorgfältig auf.
- Der BIG 10 entspricht dem aktuellen Stand der Technik und den anerkannten sicherheitstechnischen Regeln.
- Verwenden Sie beim Auspacken des Gerätes keine spitzen Gegenstände, um Beschädigungen an Gehäuse oder Kabeln zu vermeiden.
- Betreiben Sie das Gerät und die mitgelieferten Teile (Kabel usw.) nur in einwandfreiem Zustand und unter strenger Beachtung der Bedienungsanleitung.
- Arbeiten am Gerät einschließlich Öffnen des Gerätes darf nur autorisiertes Fachpersonal durchführen. Dabei sind die ESD-Schutzmaßnahmen nach DIN 100 015 zu beachten. Außer den in diesem Handbuch beschriebenen Handlungen dürfen keine Änderungen am Gerät sowie an den mitgelieferten Teilen (Kabel usw.) vorgenommen werden.
- **Achtung**: Gefährliche elektrische Spannungen! Vor Öffnen des Gerätes unbedingt Steckernetzteil ziehen und Anschlusskabel von den Schnittstellen entfernen!
- Vermeiden Sie Arbeiten am Gerät und dessen Komponenten bei Gewittertätigkeit (Trennen und Herstellen von Kabelverbindungen).
- Achten Sie beim Anschluss des Gerätes auf die richtige Netzspannung (→ Technische Daten)! Das Gerät darf nicht weiter als 1,5 Meter von der Steckdose entfernt montiert werden.
- Das Gerät besitzt keine eigene Trennvorrichtung zur Unterbrechung der Spannungsversorgung, da es für Dauerbetrieb ausgelegt ist. Achten Sie daher darauf, dass das Steckernetzteil stets leicht zugänglich ist.
- Verlegen Sie Netz- und Anschlusskabel so, dass eine Unfallgefahr durch Stolpern oder Hängen bleiben ausgeschlossen wird.
- Betreiben Sie das Gerät nur im Temperaturbereich zwischen 0°C und +45°C!
- Schützen Sie das Gerät vor direkter Sonneneinstrahlung und vor Feuchtigkeit.
- Wenn Sie das Gerät aus einer kalten Umgebung in eine wärmere Umgebung bringen, dann kann dies zu einer Betauung des Gerätes führen. Betaute Geräte dürfen nicht in Betrieb genommen werden. Warten Sie mit der Inbetriebnahme, bis das Gerät trocken ist.
- An den Schnittstellen des Modems dürfen nur Geräte angeschlossen werden, die die elektrischen Sicherheitsbestimmungen nach EN 60950 erfüllen und das CE-Zeichen tragen.
- Alle angeschlossenen Geräte müssen passende Steckverbindungen besitzen, anderenfalls sind geeignete Adapter zu verwenden.
- Alle angeschlossenen Geräte dürfen nur an den vorgesehenen Schnittstellen betrieben werden.
- Beachten Sie die Installations- und Sicherheitshinweise und halten Sie diese ein.



Safety precautions

- Please read carefully the warnings and safety precautions in this operating manual before you start installation of your BIG 10. These instructions enable you to use the full functionality of the device and to avoid damage which may result from improper use (fire, electric shock, injuries etc.). Keep this manual at a safe place.
- The BIG 10 has been manufactured according to state-of-the-art technology and complies with the generally accepted safety standards.
- Do not use sharp-edged tools for unpacking the device: they could damage cables or the enclosure.
- The device and its accessories (cable etc.) shall be operated only in faultless condition, while strictly observing these operating instructions.
- Only authorized personnel are allowed to open the enclosure and to carry out interventions in the device. Please observe the protective measures with respect to electrostatic discharge as per DIN 100 015. Manipulations on the modem or attached parts (cables etc.) other than those described in this manual are not allowed.
- **Warning**: Dangerous electric voltage! Before opening the modem, remove the plug-in power supply module and disconnect the cables from the interfaces!
- Refrain from interventions in the modem and its parts during thunderstorms (in particular, avoid plugging and unplugging of cables).
- When connecting the modem, pay attention to comply with the required mains voltage. (→ Technical data)! The device shall not be installed farther than 1.5 m from the socket.
- The device has no separate switch for interrupting the power supply, since it has been designed for continuous operation. So make sure the plug-in power supply module is always easily accessible.
- Lay the power supply and connection cables in a way to prevent accidents (such as tripping over the cables).
- The device shall be operated only between 0°C and +45°C.
- Protect the device from direct sun radiation and extreme humidity.
- When the device is taken from a cold environment into a warmer one, it may be bedewed. In this case the equipment must not be put into operation. So please wait until the modem is dry again.
- Connect to the modem interfaces only such terminal devices which meet the safety requirements acc. to EN 60950 and which are labelled with the CE symbol.
- The terminal devices shall have appropriate connectors; otherwise adequate adapters have to be used.
- Connected equipment shall only be operated at the corresponding interfaces that have been designed for them.
- Pay attention to the instructions on installation and safety and comply with them.

Sehr geehrte Kundin, sehr geehrter Kunde,

mit dem ELCONnect next BIG 10 Router haben Sie ein Gerät erhalten, welches nach dem neuesten Stand der Technik entwickelt und unter höchsten Anforderungen gefertigt wurde.

Sollte einmal etwas nicht wie beschrieben funktionieren, nehmen Sie bitte mit Ihrem Anbieter oder Händler Kontakt auf, von dem Sie dieses Gerät erworben haben. Dieser verfügt über die notwendigen Fachkenntnisse und wird Ihnen gern weiterhelfen.

Wir wünschen Ihnen viel Freude mit Ihrem BIG 10.

Verwendete Symbole

Im Bedienerhandbuch werden folgende Symbole, Formatierungsstile und Kurzhinweise verwendet:

Warnung Mit diesem Symbol wird vor Fehlbedienungen gewarnt, welche zu Problemen führen können oder Informationsverluste zur Folge haben.

Hinweis Unter unterschiedlichen Bedingungen sind vor dem Fortführen bestimmte Informationen notwendig, welche unbedingt beachtet werden sollten.

Tipp Hier finden Sie zusätzliche Tipps und Anmerkungen, welche Ihnen Arbeiten und Vorgänge durch zusätzliche Informationen erleichtern sollen.



Dear Customer,

Your ELCONnect next BIG 10 Router is a product that represents state-of-the-art technology and has been manufactured in compliance with highest quality standards.

Should it happens that something is acting up other than described, please contact your provider or salesman who has offered you the device. He will have the necessary knowledge to offer you the required support.

And now enjoy your BIG 10!

Used symbols

The manual uses the following symbols, styles and notes:

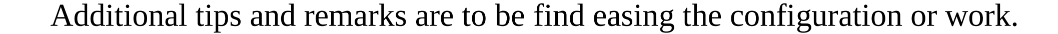
Warning This symbol warns the user of configuration mistakes leading to problems, failures or information losses.



Note Under certain condition are information necessary to take into consideration, before proceeding with the configuration.



Tipp Additional tips and remarks are to be find easing the configuration or work.





Inhalt / Contents

DEUTSCH 7

1 Technische Beschreibung des BIG 10 7
1.1 Anwendungsbereich 7
1.2 Allgemeine Merkmale 8
2 Installation 9
2.1 Hardware-Anforderungen / Systemvoraussetzungen zur Installation des BIG 10 9
2.2 Lieferumfang 9
2.3 Wahl des Montageortes / Befestigung des Gerätes 9
2.4 Anschlüsse und LEDs 10
2.5 Kabelanschluss 11
2.6 Inbetriebnahme 12
2.7 Neustart und Rücksetzen auf die Werkseinstellungen 12
2.8 Aktivierung / Deaktivierung WLAN (nur Art.-Nr. 900220) 12
2.9 Pflege und Wartung 12
2.10 Abbau des BIG 10 13
3 Konfiguration des BIG 10 über die grafische Benutzeroberfläche 13
3.1 System 16
3.1.1 Host-Name 16
3.1.2 Systemzeit 16
3.1.3 Passwort ändern 16
3.1.4 Fernadministration 16
3.1.5 Standardeinstellungen 17
3.1.6 Neustart 17
3.1.7 Firmware-Upgrade 17
3.1.8 Konfiguration laden 18
3.2 WAN 18
3.2.1 DHCP-Konfiguration 19
3.2.2 Statische Konfiguration 19
3.2.3 PPPoE 19
3.3 LAN 20
3.4 Firewall 20
3.4.1 Einstellungen 20
3.4.2 IP-Adress-Filter 20
3.4.3 MAC-Adress-Filter 21
3.4.4 DDNS 21
3.5 WLAN 21
3.5.1 Einstellungen 21
3.5.2 Sicherheit 21
3.5.3 MAC-Adress-Filter 22
3.5.4 Clients 22
3.6 Extras 22
3.7 SNMP 22
3.7.1 Grundkonfiguration 22
3.7.2 SNMPv3 Konfiguration 22
3.8 Switch 23
3.8.1 Konfiguration LAN-Ports 23



3.8.2 VLAN-Konfiguration ... 24
3.8.3 QoS-Einstellungen ... 25
3.8.4 QoS-Regeln ... 26
3.8.5 QoS-Bandbreite ... 27
3.8.6 Smart Discard ... 30
3.8.7 Port-Sicherheit ... 30
3.8.8 Statistiken ... 30
3.8.9 Monitoring ... 30
3.9 SHDSL ... 31
3.9.1 Config ... 31
3.9.2 Status ... 31
3.9.3 Performance ... 32
3.9.4 Performance History ... 32
4 Technische Daten ... 33
5 Wichtige Hinweise ... 35
5.1 Herstellererklärung ... 35
5.2 Gewährleistung ... 35
5.3 Rechte und Warenzeichen ... 35

ENGLISH ... 36

1 Technical description of the BIG 10 ... 36
1.1 Scope of application ... 36
1.2 General characteristics ... 37
2 Installation ... 38
2.1 Hardware requirements / Minimum system requirements for installation of the BIG 10 ... 38
2.2 Scope of delivery ... 38
2.3 Selecting the place of installation / Fixing the device ... 38
2.4 Interfaces and LEDs ... 39
2.5 Cable connection ... 40
2.6 Putting into operation ... 41
2.7 Restart and Factory Reset ... 41
2.8 Activation / Deactivation of WLAN (only order no. 900220) ... 41
2.9 Maintenance ... 41
2.10 Uninstallation of the BIG 10 ... 41
3 Configuration of the BIG10 router via inbuilt graphical user interface (GUI) ... 42
3.1 System ... 45
3.1.1 Host Name ... 45
3.1.2 System Time ... 45
3.1.3 Change password ... 45
3.1.4 Remote Administration ... 45
3.1.5 Default settings ... 46
3.1.6 Restart ... 46
3.1.7 Firmware upgrade ... 46
3.1.8 Import Configuration ... 47
3.2 WAN ... 47
3.2.1 DHCP Configuration ... 48

3.2.2 Static Configuration ... 48
3.2.3 PPPoE ... 48
3.3 LAN ... 48
3.4 Firewall ... 49
3.4.1 Settings ... 49
3.4.2 IP-Address Filter ... 49
3.4.3 MAC Address Filter ... 49
3.4.4 DDNS ... 49
3.5 WLAN ... 50
3.5.1 Settings ... 50
3.5.2 Safety ... 50
3.5.3 MAC Address Filter ... 50
3.5.4 Clients ... 50
3.6 Extras ... 50
3.7 SNMP ... 51
3.7.1 Basic Setup ... 51
3.7.2 SNMPv3 Setup ... 51
3.8 Switch ... 51
3.8.1 Configuration LAN Ports ... 52
3.8.2 VLAN configuration ... 53
3.8.3 QoS Settings ... 53
3.8.4 QoS Rules ... 54
3.8.5 QoS Bandwidth ... 55
3.8.6 Smart Discard ... 58
3.8.7 Port Security ... 58
3.8.8 Statistics ... 58
3.8.9 Monitoring ... 58
3.9 SHDSL ... 58
3.9.1 Config ... 58
3.9.2 Status ... 59
3.9.3 Performance ... 59
3.9.4 Performance History ... 60
4 Technical data ... 61
5 Important notes ... 63
5.1 Manufacturer´s declaration ... 63
5.2 Warranty ... 63
5.3 Rights and trademarks ... 63



DEUTSCH

1 Technische Beschreibung des BIG 10

1.1 Anwendungsbereich

Die speziellen Anforderungen heutiger Geschäftskunden an eine moderne und effiziente Kommunikationsinfrastruktur erfordern hochflexible, leistungsfähige Übertragungssysteme und Endkundengeräte. Dabei nehmen insbesondere die Forderung nach hochverfügbaren, symmetrischen Breitbanddiensten mit garantierten zugesicherten Dienstmerkmalen (SLA - Service Level Agreement) als auch die Anforderungen hinsichtlich des Bandbreitenmanagements, der Separierung der einzelnen Sprach- und Datendienste und der garantierten Verfügbarkeit bestimmter Dienste (z.B. VoIP) durch eine effiziente Priorisierung einen besonderen Stellenwert ein.

Die Produkte der Serie Business IP Gateway (BIG 10) sind speziell für die Anforderungen von Geschäftskunden entwickelt worden.

Die BIG-10-Produkte sind optimiert für Datenanwendungen wie die Übertragung von Internet-Daten, die Anbindung von Außenstellen an eine Zentrale durch den Aufbau virtueller Netze (VLAN) oder die Übertragung von Sprach- und Videodaten in Echtzeit für VoIP und Videokonferenzen. Dazu sind zahlreiche Funktionen für ein effizientes Bandbreitenmanagement und der Priorisierung von Diensten und Schnittstellen implementiert. Ein weiteres Einsatzgebiet ist die Versorgung von Mini-DSLAMs in weit entfernten Standorten, zu denen keine Glasfaserverbindung bereitgestellt werden kann. Der BIG 10 kann im Einzelbetrieb als transparente WAN-LAN-Bridge auf Schicht 2 für individuelle PCs, aber auch für Downstream-IADs, Router und DSLAMs eingesetzt werden.

Der BIG 10 verfügt über Switch- und Router-Funktion und stellt damit je nach Kundenanforderungen ein optimal abgestimmtes Gerät zur Verfügung.

Für die Übertragung der Daten zum IP-Backbone stehen bis zu 4 SHDSL-Leitungen zur Verfügung, die mittels eSHDSL-Verfahren Datenraten von bis zu 5,7 Mbit/s je Leitungspaar bereitstellen können. Durch das spezielle EFM-Bonding der SHDSL-Leitungen kann die Gesamtkapazität des Geschäftskundenanschlusses auf bis zu 22 Mbit/s erweitert werden. So lassen sich Bandbreitenerweiterungen durch Aufnahme weiterer SHDSL-Leitungen in die Bonding-Gruppe sehr einfach realisieren und Kundenwünsche nach höheren Bandbreiten schnell umsetzen.

Die hohe Verfügbarkeit des Geschäftskundenanschlusses sowie der einzelnen Dienste kann garantiert werden. Die besonderen Anforderungen an ständige Verfügbarkeit des Geschäftskundenanschlusses erfüllt das Gerät mit der optionalen Dying-Gasp-Funktion, die lokale Spannungsausfälle an den System-Administrator meldet und damit dem Netzbetreiber ermöglicht, schnell geeignete Maßnahmen zur Fehlerbeseitigung zu ergreifen.

Die lokale und Fernkonfiguration bzw. das Management wird durch das implementierte Local Craft Terminal (LCT) bzw. durch das implementierte SNMP-Protokoll gewährleistet und garantiert damit minimalen OAM-Aufwand. Die Fernverwaltung der externen SHDSL-

DSLAMs erfolgt über das implementierte EOC-Protokoll, welches bei Bedarf entsprechend angepasst werden kann.

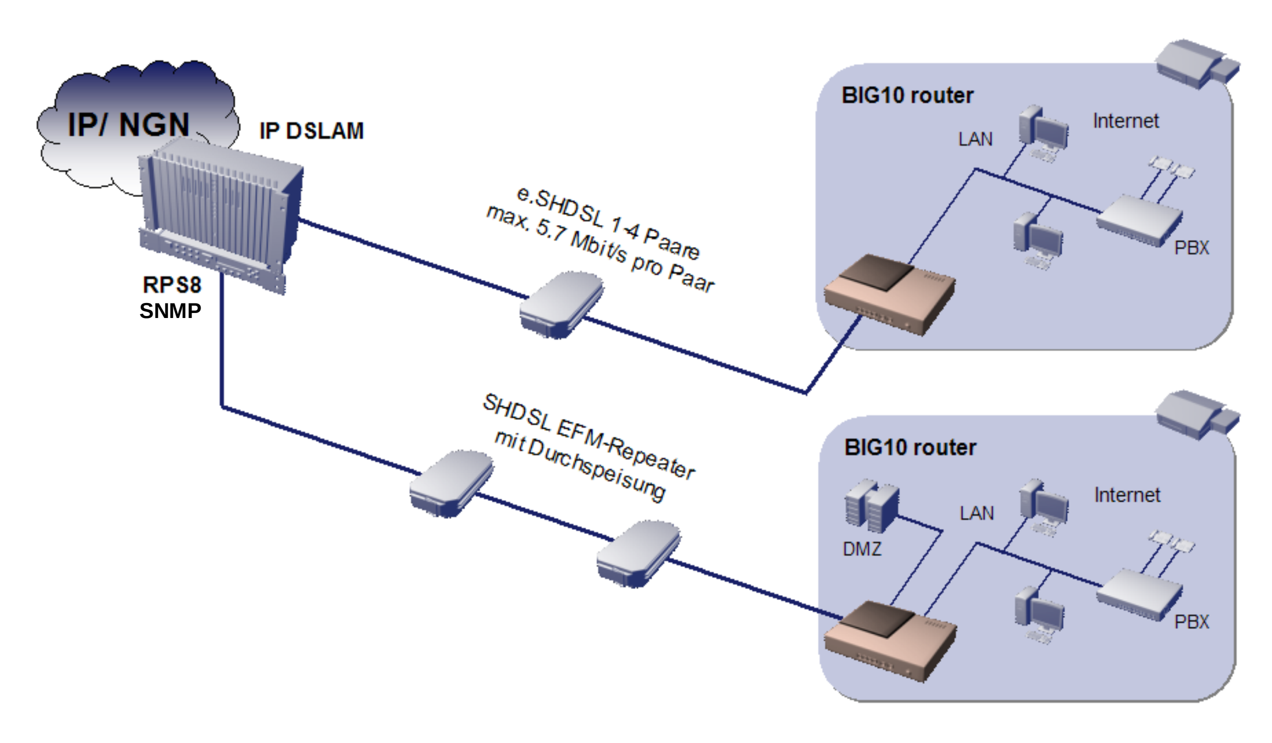


Bild 1: Anwendungsszenario allgemein

1.2 Allgemeine Merkmale

- symmetrische Datenübertragung von bis zu 22 Mbit/s über Standard-Kupferdoppeladern
- 2/4 × SHDSL-EFM mit eSHDSL und EFM-Bonding Support
- Reichweitenerhöhung durch Einsatz von bis zu 4 Repeatern oder flexible Anpassung der SHDSL-Bitrate.
- Einmessen der Kupferdoppelader und definierte Target Noise Margin durch Line Probing (PMMS)
- kundenseitige Schnittstellen
    - 4 × Ethernet
    - WLAN 802.11b/g (nur Art.-Nr. 900220)
- Switch- und Router-Support; Unterstützung von transparentem Schicht 2 - Bridging und Routing
- Betrieb als NT an externen DSLAMs
- Unterstützung von VLAN-Tagging für die Trennung von Sprach- / Datendiensten
- Unterstützung von Traffic Shaping und Priorisierung zur Gewährleistung hoher QoS
- Unterstützung von IPSec pass-through
- lokales und Fernmanagement via Grafischer Nutzeroberfläche (GUI) sowie Einbindung in 3rd-party NMS via SNMP
- Unterstützung von SNMP v1/v2/v3
- Lokalspeisung



2 Installation

2.1 Hardware-Anforderungen / Systemvoraussetzungen zur Installation des BIG 10

- Netzsteckdose mit Nennspannungsbereich 110 V … 240 V ~ / 50 Hz … 60 Hz
- Laptop oder PC mit Betriebssystem Windows® 98 SE, ME, 2000, XP; MAC; Linux und vollduplexfähiger Netzwerkkarte (Schnittstelle: 10/100Base-T); CPU: ab Pentium II®, 500 MHz
- ggf. Werkzeug für Wandmontage (Wasserwaage, Bleistift, Bohrmaschine, Bohrer Ø 6 mm, Schraubendreher)

2.2 Lieferumfang

- 1 BIG 10 Router
    - Art.-Nr. 900216: BIG 1022 (2-Port SHDSL)
    - Art.-Nr. 900217: BIG 1024 (4-Port SHDSL)
    - Art.-Nr. 900220: BIG 1044 (4-Port SHDSL / WLAN)
- 1 Steckernetzteil (12 V ⎓, 1,2 A)
- 1 Ethernetkabel, gelb, 3 m
- 1 Bohrschablone
- 1 Beutel mit Montagezubehör (2 Dübel, 2 Schrauben)
- 1 Bedienungsanleitung

2.3 Wahl des Montageortes / Befestigung des Gerätes

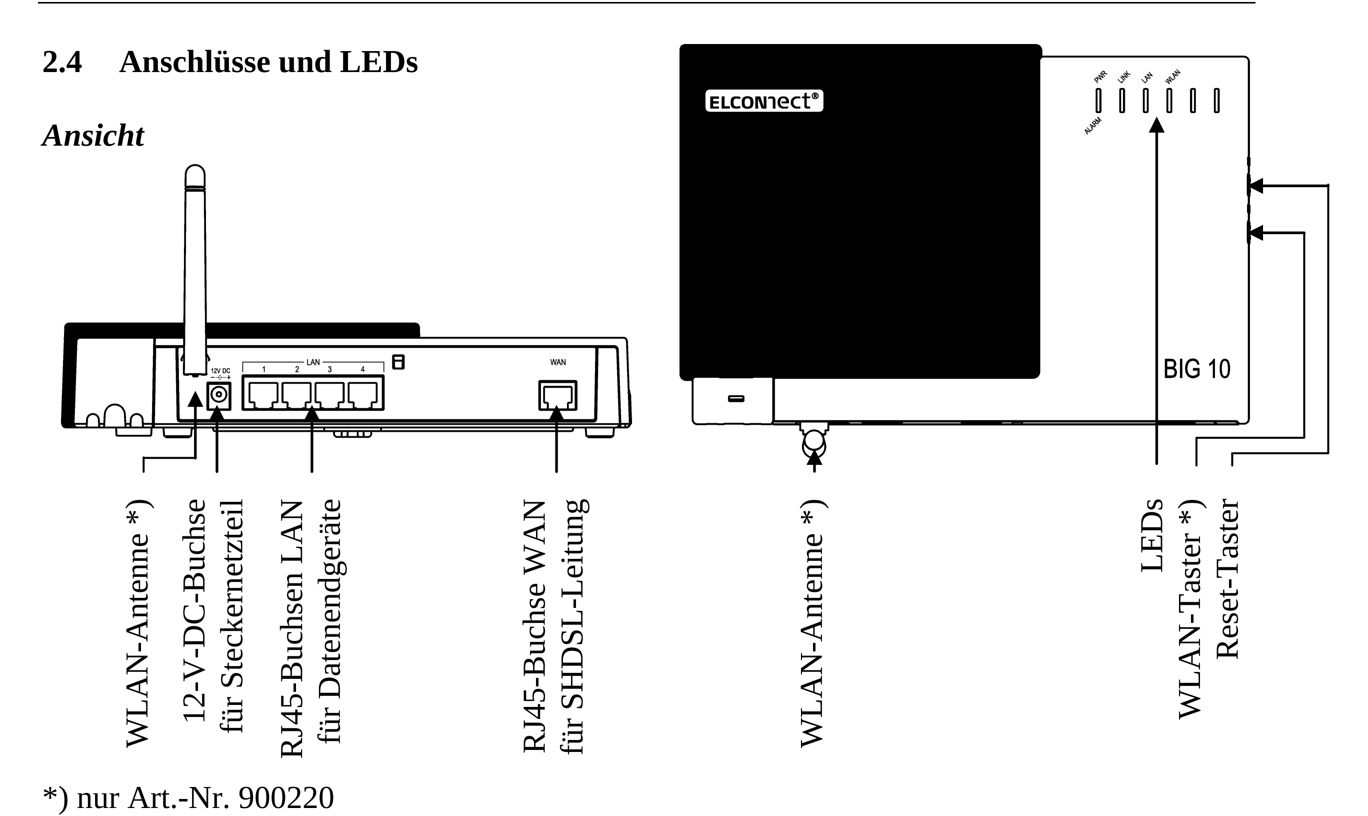
Der BIG 10 ist für den Einsatz in geschlossenen Räumen geeignet. Er kann auf den Tisch gelegt oder an der Wand befestigt werden. Installieren Sie den BIG 10 in der Nähe des DSL-Kabels. Ebenso muss sich in der Nähe des BIG 10 eine Netzsteckdose befinden. Da der BIG 10 für Dauerbetrieb ausgelegt ist, befindet sich kein Netzschalter am Gerät. Die Trennung vom Stromnetz erfolgt durch Abziehen des Steckernetzteils. Achten Sie darauf, dass das Steckernetzteil stets leicht zugänglich ist.

Stellen Sie sicher, dass bei Wandmontage an der vorgesehenen Montagestelle keine Leitungen (Strom, Wasser, Gas, Telefon, Koaxialkabel, Glasfaser) unter Putz verlegt sind. Während des Betriebs entwickelt der BIG 10 eine fühlbare, aber völlig ungefährliche Betriebstemperatur. Um eine ungehinderte Wärmeableitung zu gewährleisten, darf der BIG 10 nicht in Gehäuse ohne ausreichende Wärmeableitung eingebaut werden. Ebenfalls aus diesem Grund ist das Gerät auch vor intensiver Wärmeeinwirkung, z.B. durch Heizkörper oder Sonneneinstrahlung zu schützen. Halten Sie Feuchtigkeit vom BIG 10 fern. Vermeiden Sie eine sehr staubhaltige Umgebung.

Die Montagehinweise finden Sie direkt auf der Bohrschablone.

2.4 Anschlüsse und LEDs

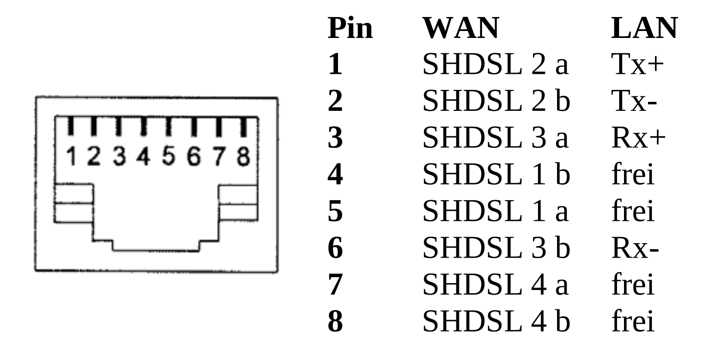
Ansicht



*) nur Art.-Nr. 900220

Bild 2: Ansicht des BIG 10

Pinbelegung der RJ45-Buchsen (WAN, LAN)



Pin	WAN	LAN
1	SHDSL 2 a	Tx+
2	SHDSL 2 b	Tx-
3	SHDSL 3 a	Rx+
4	SHDSL 1 b	frei
5	SHDSL 1 a	frei
6	SHDSL 3 b	Rx-
7	SHDSL 4 a	frei
8	SHDSL 4 b	frei

Bild 3: Pinbelegung der RJ45-Buchsen

LED-Signalisierung

Das Modem verfügt über 4 (5) LEDs, die über die Aktivitäten der Datenübertragung Auskunft geben.

LED	Farbe	Status	Bedeutung
PWR Status Stromversorgung	gelb	AUS	keine Netzspannung vorhanden
		AN	Netzspannung vorhanden
ALARM Status Alarm	rot	AUS	keine wichtige Alarmmeldung empfangen
		blinkt	Geräte-Initialisierung nach Einschalten, bis Gerät betriebsbereit ist
		AN	wichtige Alarmmeldung empfangen oder nach Reset, bis Gerät wieder betriebsbereit



LED	**Farbe**	**Status**	**Bedeutung**
LINK Status SHDSL	grün	AUS	WAN-Verbindung nicht hergestellt
		blitzt	Datenübertragung über min. eine SHDSL
		AN	Alle PCS-Teilnehmer sync; WAN-Verbindung hergestellt
	gelb	AUS	WAN-Initialisierung erfolgt; alle Verbindungen down; alle PCS-Teilnehmer sync; keine Beeinträchtigung des eingestellten Zustandes
		AN	Schnellste Verbindung PCS sync, noch nicht alle Teilnehmer sync; Beeinträchtigung des eingestellten Zustandes vorhanden
		blitzt (langsam)	Verbindungs-ID (1…4) schnellste Verbindung G.hs-Transfer (max. 4 ON-Impulse innerhalb 2 Sekunden)
		blitzt (invers)	Schnellstes link line probing
		blinkt mit 1 Hz	Schnellste data link Training; „SHDSL Training“ Status
		blinkt mit 2 Hz	Schnellster data link-Modus; „Line Probing“ Status
		blinkt mit 4 Hz	(Neu-)initialisierung läuft; „G.hs“ Status
LAN Status LAN	grün	AUS	keine Verbindung zu einem LAN-Port
		blitzt (invers)	Datenübertragung über min. einen LAN-Port
		AN	Verbindung zu min. einem LAN-Port hergestellt
	gelb	AUS	keine Beeinträchtigung des eingestellten Zustandes
		AN	Beeinträchtigung des eingestellten Zustandes vorhanden
WLAN (nur Art.-Nr. 900220) Status WLAN	blau	AUS	WLAN deaktiviert
		blitzt (invers)	Datenübertragung über WLAN
		AN	WLAN aktiviert
	gelb	AUS	keine Beeinträchtigung des eingestellten Zustandes
		blinkt	nach Einschalten, bis WLAN-Access-Point betriebsbereit
		AN	Initialisierung / Beeinträchtigung des eingestellten Zustandes vorhanden

2.5 Kabelanschluss

1. Verbinden Sie die WAN-Schnittstelle des BIG 10 mit dem Zugang Ihres Netzbetreibers. Benutzen Sie für eine optimale Übertragung ein UTP (Unshielded Twisted Pair) CAT5-Kabel oder besser. Die Kabelbelegung der Anschlussdose erfahren Sie von Ihrem Netzanbieter.

2. Verbinden Sie den BIG 10 mit der Netzwerkkarte des PCs. Nutzen Sie dafür ein Ethernet-Kabel und schließen es an eine der mit „LAN“ gekennzeichneten RJ45-Buchsen des BIG 10 und an die RJ45-Buchse der Netzwerkkarte an (siehe deren Anleitung).
3. Zuletzt verbinden Sie die Buchse „12V DC“ des BIG 10 mithilfe des beiliegenden Steckernetzteils mit dem Stromnetz. Verwenden Sie ausschließlich das im Lieferumfang enthaltene Steckernetzteil. Die Verwendung anderer Netzteile führt zum Verlust der CE-Konformität und zum Ausschluss der Gewährleistung.

2.6 Inbetriebnahme

Mit Anliegen der Speisespannung und nach erfolgter Autokonfiguration ist der BIG 10 betriebsbereit. Die gesamte Verbindung des Zugangsnetzes bis zum BIG 10 wird vom Netzbetreiber in Betrieb genommen und ist vorkonfiguriert bzw. konfiguriert sich durch Autokonfiguration selbst.
Voraussetzung für die Inbetriebnahme der Datenverbindung über das BIG 10 ist eine korrekte Installation der Netzwerkkarte Ihres PCs. Nähere Hinweise dafür entnehmen Sie bitte den Unterlagen des Herstellers der Netzwerkkarte. Für weitere Fragen bzgl. der Konfiguration Ihres PC wenden Sie sich bitte an Ihren Dienstanbieter.

2.7 Neustart und Rücksetzen auf die Werkseinstellungen

Sollte sich das BIG 10 in einem undefinierten Betriebszustand befinden (z.B. wenn keine Datenübertragung möglich ist), kann ein kurzes Drücken des Reset-Tasters das Gerät neu starten und die Datenverbindung neu aufbauen. Der Reset-Taster befindet sich auf der rechten Gehäuseseite. Um den Neustart auszuführen, betätigen Sie den Reset-Taster ca. 1 s mit einem spitzen Gegenstand (z.B. Kugelschreiber oder Büroklammer). Kontaktieren Sie in jedem Fall zuvor Ihren Dienstanbieter. Ein langer Druck auf den Reset-Taster (> 5 s) verursacht ein Rückstellen des Gerätes auf die Werkseinstellungen, d.h. alle vorgenommenen Einstellungen gehen verloren. Ein Rücksetzen auf die Werkseinstellungen sollte nur von versierten Nutzern vorgenommen werden. Ein Rücksetzen kann zur Funktionsunfähigkeit des BIG 10 führen! Kontaktieren Sie deshalb in jedem Fall zuvor Ihren Dienstanbieter!

2.8 Aktivierung / Deaktivierung WLAN (nur Art.-Nr. 900220)

Nach der ersten Inbetriebnahme des Gerätes ist das WLAN-Modul deaktiviert. Sie können das WLAN-Modul durch Drücken des WLAN-Tasters aktivieren. Der Taster befindet sich auf der rechten Gehäuseseite unter dem Reset-Taster.
Ein erneutes Drücken des WLAN-Tasters deaktiviert das WLAN-Modul wieder. Der jeweilige Zustand wird Ihnen durch die WLAN-Status-LED signalisiert.

2.9 Pflege und Wartung

Ihr BIG 10 ist wartungsfrei. Die Reinigung erfolgt mit einem trockenen Tuch. Verwenden Sie niemals scheuernde oder ätzende Reinigungsmittel.



Ziehen Sie das Steckernetzteil aus der Steckdose bzw. nehmen Sie das Gerät während der Reinigung außer Betrieb.



2.10 Abbau des BIG 10

Zum Abbau des BIG 10 lösen Sie zunächst sämtliche Kabel, beginnend mit dem Steckernetzteil. Jetzt kann das Gerät von der Wand abgenommen werden.

3 Konfiguration des BIG 10 über die grafische Benutzeroberfläche

Der BIG 10 kann komfortabel über eine eingebaute grafische Benutzeroberfläche konfiguriert werden. Dies geschieht über Web-Browser (Firefox, Internet Explorer, Safari), die mittlerweile auf den meisten modernen Computern verfügbar sind.
Um auf die Web-Oberfläche zuzugreifen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass die Netzwerkeinstellungen Ihres Computers ein automatisches Beziehen der IP-Adresse zulassen. Fragen Sie ggf. Ihren Netzwerkadministrator, um die Einstellungen vorzunehmen.
2. Verbinden Sie die LAN-Schnittstelle Ihres Computers mit einer LAN-Buchse des BIG 10 mittels eines LAN-(Ethernet-)Kabels.
3. Nach Anschluss des BIG 10 am Computer wird diesem eine IP-Adresse automatisch zugewiesen.

Es ist ebenfalls die Einstellung einer festen IP-Adresse möglich. Weisen Sie dazu Ihrem Computer folgende Daten zu:

	Voreinstellung	**Benutzereinstellung**
Adressbereich	192.168.1.2 bis 255	
Subnetzmaske	255.255.255.0	
Gateway-Adresse	192.168.1.1	

Öffnen Sie jetzt den Web-Browser Ihres Computers und tragen Sie in die Adresszeile folgendes ein: http://192.168.1.1



Hinweis Stellen Sie sicher, dass Ihre Proxy-Einstellungen korrekt sind.



Nach erfolgreichem Verbindungsaufbau erscheint das Login-Fenster.

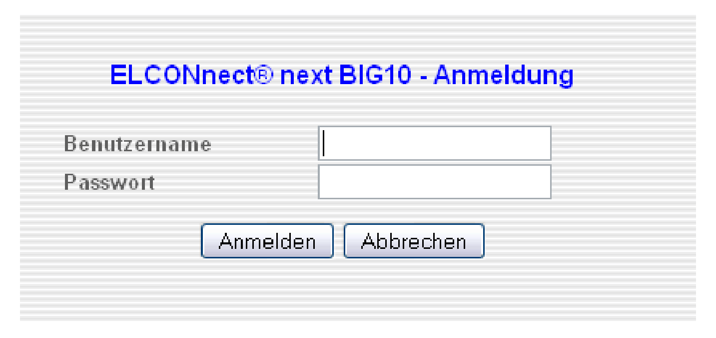


Bild 4: Anmeldefenster

Die Anmeldung erfolgt über folgende Benutzer:

- Ein „normaler Nutzer“ kann hauptsächlich Statusinformationen des Gerätes einsehen.
- Ein „erweiterter Nutzer“ kann sämtliche Einstellungen des Gerätes vornehmen.

Benutzer		**Voreinstellung**	**Benutzereinstellung**
normaler Nutzer	Benutzername	admin	
	Passwort	admin	
erweiterter Nutzer	Benutzername	isp-admin	
	Passwort	isp-admin	

Nach erfolgreicher Anmeldung erhalten Sie nach einigen Sekunden einen Überblick über den System-Status. In dieser Übersicht werden die Netzwerk-Konfigurationen und der aktuelle Firmware-Stand angezeigt.

elcon systemtechnik V0.15 1

2 Startseite | System-Status | (isp-admin) Abmelden
Konfigurationsassistent | Erweiterte Konfiguration

System-Status

Diese Seite gibt Ihnen einen schnellen Überblick über die Netzwerk-Konfiguration und den momentanen Verbindungsstatus Ihres ELCONnect® next BIG10.

WAN (Internet)	Management (geändert)	Data (geändert)
IP-Adresse	0.0.0.0	0.0.0.0
Subnetz-Maske	0.0.0.0	0.0.0.0
Standard-Gateway	0.0.0.0	0.0.0.0
DNS-Server 1	0.0.0.0	0.0.0.0
DNS-Server 2	0.0.0.0	0.0.0.0
Verbindungstyp		
VLAN-ID	n.a.	n.a.
WAN MAC-Adresse	00:07:23:09:03:40	

LAN (Gateway)	
Netzwerkmodus	restricted
IP-Adresse	192.168.1.1
Subnetz-Maske	255.255.255.0
DHCP-Server	Aktiviert
Firewall	Aktiviert
LAN MAC-Adresse	00:07:23:09:03:41

Port	Link	Mode	Flow Control	Auto Negotiation	MDI-Mode
LAN1	Up	100Mb/s Full Duplex	Deaktiviert	Aktiviert	MDI
LAN2	Down	?	?	Aktiviert	?
LAN3	Down	?	?	Aktiviert	?
LAN4	Down	?	?	Aktiviert	?
WAN	Down	?	?	Aktiviert	----

Allgemeine Informationen	
Firmware-Version	VA_A900217_S800_C049FM_V020.42

Bild 5: System-Status

Für die weitere Navigation innerhalb der Benutzeroberfläche sind folgende rot gekennzeichnete Bereiche wichtig:



(1) Umschalten der Sprache; voreingestellt ist Deutsch

(2) Basis-Menüs; folgende Menüs sind vorhanden:

I. Startseite: hiermit gelangen Sie aus jedem Menü zu dieser oben angezeigten Seite
II. System-Status: hiermit gelangen Sie aus jedem Menü zu dieser oben angezeigten Seite
III. (angemeldeter Benutzer) Abmelden: zeigt den angemeldeten Nutzer und meldet diesen vom System ab; die Anzeige spring zum Login-Fenster
IV. Konfigurationsassistent: der Assistent führt Sie durch die wichtigsten Einstellungen
V. Erweiterte Konfiguration: hiermit gelangen Sie zur manuellen, menügeführten Konfiguration

Im Folgenden werden Ihnen noch weitere wichtige Navigationselemente gezeigt:

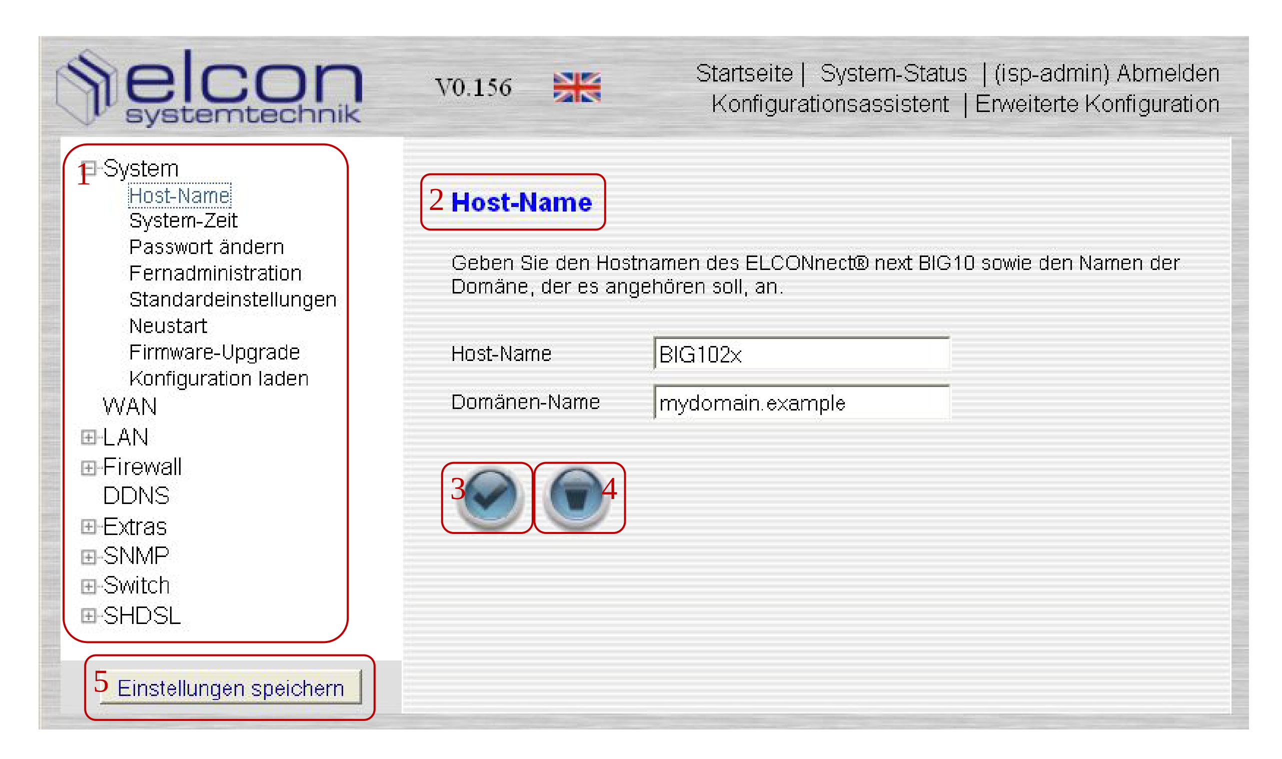


Bild 6: Navigationselemente

(1) Menü zur manuellen Konfiguration des BIG 10
Die Menüpunkte enthalten Unterpunkte, die durch Anklicken des Menüpunktes sichtbar werden. Der jeweils ausgewählte Menü- oder Unterpunkt wird blau dargestellt.

(2) Anzeige des gewählten Menü- oder Unterpunktes

(3) Button zum Bestätigen der jeweils getätigten Eingabe

(4) Button zum Löschen der jeweils getätigten Eingabe

(5) Button zum Bestätigen aller getätigten Eingaben

Hinweis



Zum Übernehmen der Änderungen an der Konfiguration des BIG 10 müssen Sie abschließend auf den "Einstellungen speichern"-Button klicken. Dieser Schritt ist unbedingt erforderlich, da sonst die von Ihnen getätigten Einstellungen beim nächsten Neustart des BIG 10 verloren gehen würden!

3.1 System

In diesem Menü nehmen Sie die systemspezifischen Einstellungen Ihres BIG 10 vor.

3.1.1 Host-Name

Geben Sie hier den Hostnamen des BIG 10 sowie den Namen der Domäne, der es angehören soll, an. Beide Einträge sind optional.

3.1.2 Systemzeit

Abhängig von der gewählten Zeitzone synchronisiert der BIG 10 die Systemzeit mit einem NTP- (Network Time Protocol) Server im Internet. Die korrekte Uhrzeit ist unter anderem notwendig, damit im System-Log die Einträge mit dem korrekten Datum und der korrekten Uhrzeit angezeigt werden.

3.1.3 Passwort ändern

Der Zugriff auf die Konfigurations-Oberfläche des BIG 10 ist durch ein Passwort geschützt. In diesem Menü können Sie das voreingestellte Passwort oder auch den Zugangsnamen ändern.

Die Zeit bis zum automatischen Abmelden gibt die Zeitdauer an, bis zu der der Zugriff auf die Web-Oberfläche aus Sicherheitsgründen gesperrt wird. Nach Ablauf dieser Zeit müssen Sie erneut Ihren Benutzernamen und das zugehörige Passwort eingeben.

3.1.4 Fernadministration

Wenn Sie das BIG 10 auch von außerhalb Ihres lokalen Netzwerks über das Internet administrieren wollen, müssen Sie die Fernadministration aktivieren. Der Zugriff kann dabei auf eine angegebene IP-Adresse oder einen IP-Adressbereich eingeschränkt werden. Die Angabe von einem "*" in allen IP-Adressfeldern bedeutet, dass WAN-seitig von jeder beliebigen IP-Adresse aus eine Verbindung zum BIG 10 aufgebaut werden kann. Wenn Sie IP-Adressbereiche zulassen wollen, müssen Sie in die entsprechenden IP-Adressfelder das Zeichen "*" eintragen. Dabei ist zu beachten: Wenn ein IP-Adressfeld das Zeichen "*" enthält, müssen alle rechts davon gelegenen IP-Adressfelder ebenfalls das Zeichen "*" enthalten.
Für den Fernzugriff auf die Benutzeroberfläche des Gerätes müssen Sie zusätzlich zur IP-Adresse die Portnummer in der Art „http://IP-Adresse:Portnummer“ angeben. Diese ist konfigurierbar im Bereich von 1024 – 65535.

Beispiel



Die Eingabe „217.63.*.*“ bedeutet, dass alle Computer mit der IP-Adresse zwischen 217.63.0.0 und 217.63.254.254 Zugriff auf das Gerät haben. Ist die Portnummer 8080 konfiguriert, ist folgende Eingabe im Browser zu tätigen: „http://217.63.0.1:8080“.

Möchten Sie mehr als einen Bereich zur Fernadministration konfigurieren, können Sie dies über eine Konfigurationsdatei realisieren. Verwenden Sie dazu die Hinweise in Kapitel 3.2.



3.1.5 Standardeinstellungen

Falls die Konfiguration das Gerät in einen nicht funktionierenden Zustand versetzt hat, können Sie den Auslieferungszustand (Standardeinstellungen) wieder herstellen. Zwei Stufen des Zurücksetzens sind möglich:

- „User Parameter zurücksetzen“ setzt alle vom Nutzer „admin“ einstellbaren Werte auf die Standardeinstellungen zurück.
- „Zurücksetzen auf Werkseinstellungen“ setzt alle einstellbaren Werte des Gerätes auf die Standardeinstellungen zurück.

Klicken Sie auf den jeweiligen Button, um die Standardeinstellungen zu setzen. Sie müssen die Wiederherstellung der Standardeinstellungen anschließend noch einmal bestätigen.

Warnung Alle Einstellungen werden auf ihre Standardwerte zurückgesetzt! Wollen Sie das wirklich?

3.1.6 Neustart

Für den Fall, dass der BIG 10 nicht mehr korrekt reagiert oder in irgendeiner Form nicht mehr korrekt arbeitet, können Sie einen Neustart ausführen. Ihre Einstellungen werden dabei nicht geändert. Um den Neustart auszulösen, klicken Sie auf den „Neustart“-Button.
Ein Neustart wird ebenfalls über den seitlich am Gerät verdeckt angebrachten „Reset“-Taster ausgeführt. Siehe dazu Kapitel 2.7.

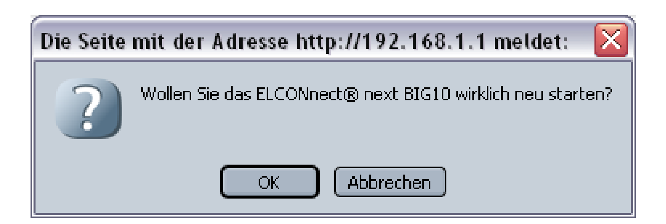


Bild 7: Sicherheitsabfrage bei Neustart

3.1.7 Firmware-Upgrade

Das Gerät unterliegt einer ständigen Verbesserung der Funktionalität oder Leistungsfähigkeit. Sobald eine neue Software (Firmware) zur Verfügung steht, können Sie diese in das Gerät laden. Gehen Sie dazu wie folgt vor:

1. Bitte speichern Sie die Firmware zunächst auf Ihrem Rechner.
2. Klicken Sie auf „Durchsuchen“, geben Sie den Pfad und Dateinamen der Firmware-Datei an und klicken Sie auf den Anwenden-Button. Wollen Sie das Gerät nach dem Firmware-Update auf die Werkseinstellungen zurücksetzen, dann markieren Sie die entsprechende Option.
3. Sie werden anschließend noch einmal aufgefordert das Firmware-Upgrade zu bestätigen.



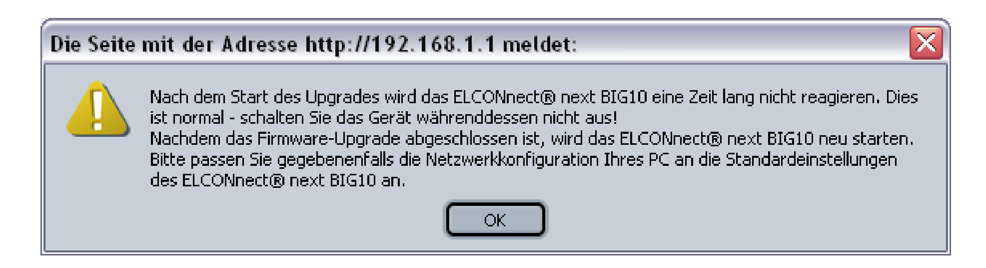


Bild 8: Hinweis bei Firmware-Upgrade

4. Danach erscheinen folgende Meldungen, die Sie unbedingt beachten sollten:

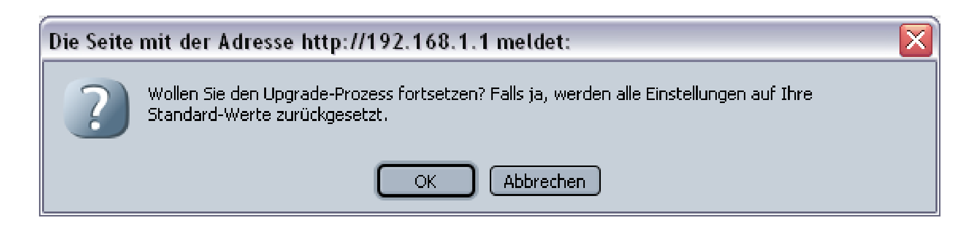


Bild 9: Sicherheitsabfrage bei Firmware-Upgrade

Hinweis



Der Firmware-Upgrade ändert nicht die Konfiguration des BIG 10. Alle Einstellungen werden beibehalten. Sichern Sie trotzdem vorher die Einstellungen!

3.1.8 Konfiguration laden

Falls Sie mehrere Geräte des gleichen Typs BIG 10 identisch konfigurieren möchten, können Sie dies über eine Konfigurationsdatei vornehmen. Dies ist von einem zentralen Server aus möglich, wie im nächsten Kapitel beschrieben, oder lokal über die Konfigurationsoberfläche. Bereiten Sie dazu die Konfigurationsdatei vor. Dazu gehen Sie vor wie in der Dokumentation „Konfiguration-Documentation“ beschrieben. Die Konfigurationsdatei kann über einen einfachen Texteditor geschrieben werden.
Laden Sie nun diese Datei in das Gerät. Wenn die Konfiguration wie gewünscht funktioniert, dann aktivieren Sie zusätzlich die Option „Konfiguration dauerhaft speichern“. Danach bleibt die Konfiguration auch nach einem Neustart des Gerätes erhalten.

3.2 WAN

Die WAN-Seite des Routers kann auf verschiedene Art und Weise konfiguriert werden. Dabei kann der Management-Pfad vom allgemeinen Datenpfad getrennt werden, um die Konfiguration des Gerätes in einem gesicherten Bereich vornehmen zu können.
Konfigurieren Sie zuerst Bereiche für die Netzwerkkonfiguration. Diese können sich in separaten VLANs befinden und unterschiedliche Konfigurationstypen aufweisen. Diesen können sein:

- dynamische Konfiguration („DHCP“), welche eine IP-Adresse von einem im Netz befindlichen DHCP-Server erhält
- statische Konfiguration mit einer konfigurierten, festen IP-Adresse
- IP-Adressvergabe über PPPoE



Zusätzlich kann das Laden einer Konfigurationsdatei von einem zentralen TFTP-Server in das Gerät ermöglicht werden. Dazu ist „Opt. 66/67“ auszuwählen. Somit kann auf einfache Weise eine zentrale Gerätekonfiguration erzielt werden.

Warnung Ist die tftp-Serveradresse nicht erreichbar oder kann die Konfigurationsdatei nicht geladen werden, dann führt das Gerät ein automatisches Reset durch und startet neu. Dies wird in zyklischen Abständen wiederholt.

Wenn Sie die Netzwerkkonfiguration vorgenommen haben, weisen Sie jetzt dem Management-Pfad und dem Datenpfad jeweils eine Konfiguration zu.
Schließlich können Sie noch angeben, in welchem Pfad sich Ihr(e) DNS-Server befindet(n) und können diese(n) konfigurieren.

3.2.1 DHCP-Konfiguration

Mit der WAN-Einstellung „DHCP“ wird dem Gerät per DHCP eine IP-Adresse dynamisch vergeben.

3.2.2 Statische Konfiguration

Bei der Einstellung „Statisch“ müssen Sie IP-Adresse, Subnetzmaske, Gateway und DNS-Server von Hand konfigurieren. Wählen Sie „Statisch“, wenn Ihr Internetprovider Ihnen die erforderlichen Daten zur Verfügung gestellt hat. Mit der Einstellung „Statisch“ ist nur eine Vergabe fester IP-Adressen möglich; DHCP wird hierbei nicht unterstützt.

Warnung Wenn Sie auf dieser Seite Änderungen vornehmen, führt das dazu, dass beim nächsten Klick auf den Button "Einstellungen speichern" automatisch ein Neustart des BIG 10 eingeleitet wird.

3.2.3 PPPoE

Bei der Einstellung "PPPoE" werden IP-Adresse, Subnetzmaske, Gateway und DNS-Server zentral vergeben. Wählen Sie "PPPoE", wenn Ihr Internetprovider Ihnen die erforderlichen Zugangsdaten und Passwort zur Verfügung gestellt hat.
Die Eingabe der PPPoE-Daten erfolgt in einem separaten Menüeintrag „WAN PPPoE“. Dieser ist verfügbar, sobald Sie PPPoE gewählt und diese Auswahl gespeichert haben.
Geben Sie hier Ihre PPPoE-Zugangsdaten ein. Da das Passwort bei der Eingabe nicht im Klartext dargestellt wird, müssen Sie das Passwort wiederholen, um eine Fehleingabe zu erkennen. Die Daten für „Service Name“ / „Service Concentrator“ sind optional, falls diese Daten Ihnen zur Verfügung gestellt wurden.
Ebenfalls können Sie zwischen der Verbindungsart „permanent“ oder „on demand“ wählen. Bei „on demand“ geben Sie unter „Maximum Idle Time“ eine maximale Zeitperiode ein, in welcher die Internetverbindung bei Inaktivität erhalten bleibt. Wenn die Verbindung für eine größere Zeitperiode inaktiv ist, wie in „Maximum Idle Time“ definiert, wird die Verbindung getrennt.

3.3 LAN

In diesen Menüs erfolgt die Konfiguration der LAN-Schnittstelle des BIG 10 und des DHCP-Servers für Ihr lokales Netzwerk.

Der BIG 10 hat für das lokale Netz eine voreingestellte IP-Adresse, welche in diesem Menü verändert werden kann. Um den an den LAN-Schnittstellen angeschlossenen Geräten automatisch eine IP-Adresse zuzuweisen, können Sie den eingebauten DHCP-Server aktivieren. Der IP-Adressbereich des DHCP-Servers und die Gültigkeitsdauer (Lease-Gültigkeit) der vergebenen IP-Adresse können verändert werden. Ebenso ist optional die Konfiguration einer Domäne unter Angabe des Domänennamens möglich.

3.4 Firewall

Der BIG 10 kann Ihr Netzwerk mit einer Firewall schützen, sodass sich das Gerät mit dann eingeschränkten Verbindungsparametern erfolgreich gegen eine Vielzahl bekannter Hacker-Angriffe verteidigen kann. Um trotzdem noch von außerhalb auf einen oder mehrere der lokalen PCs zugreifen zu können, müssen Sie dies im Abschnitt NAT konfigurieren. Für zusätzlichen Schutz sorgen Einstellungen, die von Hackern gern genutzte Methoden zur Vorbereitung eines Angriffs unterbinden. Außerdem können Sie Client-PCs den Internet-Zugriff ganz oder teilweise verbieten.

3.4.1 Einstellungen

Die Firewall muss aktiviert sein, bevor der BIG 10 Ihr Netzwerk vor Angriffen aus dem Internet schützen kann. Zusätzlich können Sie aber auch noch einige spezielle Schutzmechanismen aktivieren: Das Deaktivieren der Optionen „PING von WAN erlauben“ und „PING von LAN erlauben“ verhindert, dass der BIG 10 auf Ping-Pakete aus dem Internet bzw. aus dem lokalen Netzwerk antwortet. „Portscans verhindern“ blockiert das Scannen der Ports aus dem Internet.

3.4.2 IP-Adress-Filter

Sie können Client-PCs abhängig von ihrer IP-Adresse und je nach gewähltem Portnummern-Bereich ganz oder teilweise den Zugriff auf das Internet sperren. Wenn Sie statt eines Bereichs nur eine bestimmte IP-Adresse oder Portnummer angeben möchten, geben Sie zweimal dieselbe Nummer an (Beispiel: 192.168.1.1 ~ 1). Als Portnummer können Sie eine Zahl zwischen 1 und 65535 eingeben.

Hinweis Die Option IP-Adress-Filter lässt sich nur bei eingeschalteter Firewall aktivieren.





3.4.3 MAC-Adress-Filter

Sie können am LAN angeschlossenen Computern, abhängig von ihrer MAC-Adresse, den Zugriff auf das Internet verhindern. Dazu aktivieren Sie die Funktion „MAC-Adress-Filter“ und geben die MAC-Adresse des Datengerätes ein.

Hinweis Der MAC-Adress-Filter lässt sich nur bei eingeschalteter Firewall aktivieren.



3.4.4 DDNS

DDNS (Dynamic Domain Name System) ermöglicht bei dynamisch zugewiesener WAN-IP-Adresse, dass das BIG 10 immer unter demselben Host-Namen erreichbar ist. Es sind verschiedene DynDNS-Anbieter vorkonfiguriert. Konsultieren Sie diese Anbieter, um die notwendigen Einstellungen zu erfahren.

3.5 WLAN

Hier können Sie Ihre WLAN-Basisstation konfigurieren.

Hinweis Zum Übernehmen der Änderungen an der Konfiguration des BIG 10 müssen Sie abschließend auf den "Einstellungen speichern"-Button klicken. Dieser Schritt ist unbedingt erforderlich, da sonst die von Ihnen getätigten Einstellungen beim nächsten Neustart des BIG 10 verloren gehen würden!



3.5.1 Einstellungen

Hier können Sie die Grundeinstellungen der WLAN-Basisstation vornehmen. Mit „Wireless LAN aktivieren” können Sie die WLAN-Basisstation ein- bzw. ausschalten. Sie können den WLAN-Netzwerknamen festlegen bzw. die Übertragung des Namens ein- bzw. ausschalten.

3.5.2 Sicherheit

Hier legen Sie die Sicherheitseinstellungen der WLAN-Basisstation fest. Sie können den Verschlüsselungsstandard und Ihren persönlichen WLAN-Schlüssel festlegen. Ebenso können Sie festlegen, ob die Authentisierung lokal (PSK) oder über einen zentralen Server (Radius) erfolgen soll.

Hinweis Verschlüsseln Sie immer Ihr WLAN-Netzwerk! Missbrauch über ein unverschlüsseltes Netzwerk kann rechtliche Folgen nach sich ziehen.
Verschlüsseln Sie möglichst Ihr Netzwerk mit dem stärksten Verschlüsselungsverfahren WPA2, da andere Verschlüsselungsverfahren unsicher sind.



3.5.3 MAC-Adress-Filter

Um ein Mindestmaß an Sicherheit zu erzielen, können Sie auf dieser Seite MAC-Adressen, von denen aus der Zugriff auf Ihr WLAN erlaubt bzw. verboten ist, angeben.

Hinweis MAC-Adressen können leicht gefälscht werden. Daher stellt dieser Filter kein wirkliches Sicherungsverfahren dar.



3.5.4 Clients

In dieser Liste sehen Sie die MAC-Adressen der Clients, die mit Ihrem WLAN verbunden sind.

3.6 Extras

In bestimmten Netzwerkkonfigurationen ist es notwendig, ausgehenden IP-Paketen, welche geroutet werden, mit einem neuen DSCP-Wert zu versehen („remarking“). Dazu stehen im BIG 10 zwei verschiedene Verfahren zur Verfügung. Unter „aktiv“ können Sie entsprechende DSCP-Werte setzen.
Nutzen Sie die Auswahl „erweitert“, um bis zu 20 entfernten Router (oder anderen Netzwerkgeräten) über deren IP-Adresse einen individuellen DSCP-Wert zu konfigurieren.

3.7 SNMP

Das Simple Network Management Protocol (SNMP) unterstützt den Austausch von Nachrichten zwischen einem Netzwerkmanagement-Client und einem Netzwerkmanagement-Agenten zum zentralen Verwalten von Netzelementen.
Diese Nachrichten beinhalten Anforderungen („requests“), um Variablen zu setzen („set“) und zu erhalten („get“), welche in Netzelementen existieren, um Statistiken zu erhalten, Konfigurationsparameter zu setzen und Ereignisse im Netzwerk zu beobachten. SNMP kann nur über das WAN kommunizieren. Der BIG 10 kann sog. SNMP traps erzeugen, um Alarmzustände zu signalisieren.
Der BIG 10 besitzt für das Geräte-Netzwerkmanagement einen SNMP-Agenten. Auf der Gegenseite ist dafür ein MIB-Browser erforderlich, der die SNMP-Versionen v1/v2/v3 unterstützt.

3.7.1 Grundkonfiguration

Zum Export von BIG 10-Funktionen zum MIB-Browser müssen Sie die SNMP-Server-Einstellungen aktivieren.

3.7.2 SNMPv3 Konfiguration

Der BIG 10 bietet mittels SNMPv3 Sicherheit beim SNMP-Zugriff. Sie können SNMPv3 aktivieren und so konfigurieren, dass die Nutzer autorisierten Zugriff zu den SNMP-Daten haben.



3.8 Switch

In diesem Abschnitt können Sie den LAN-Switch Ihres BIG 10 konfigurieren. Die Switch-funktionalität wird über innere und nach außen geführte Ports bestimmt. Das folgende Bild zeigt diese Portzuordnung:

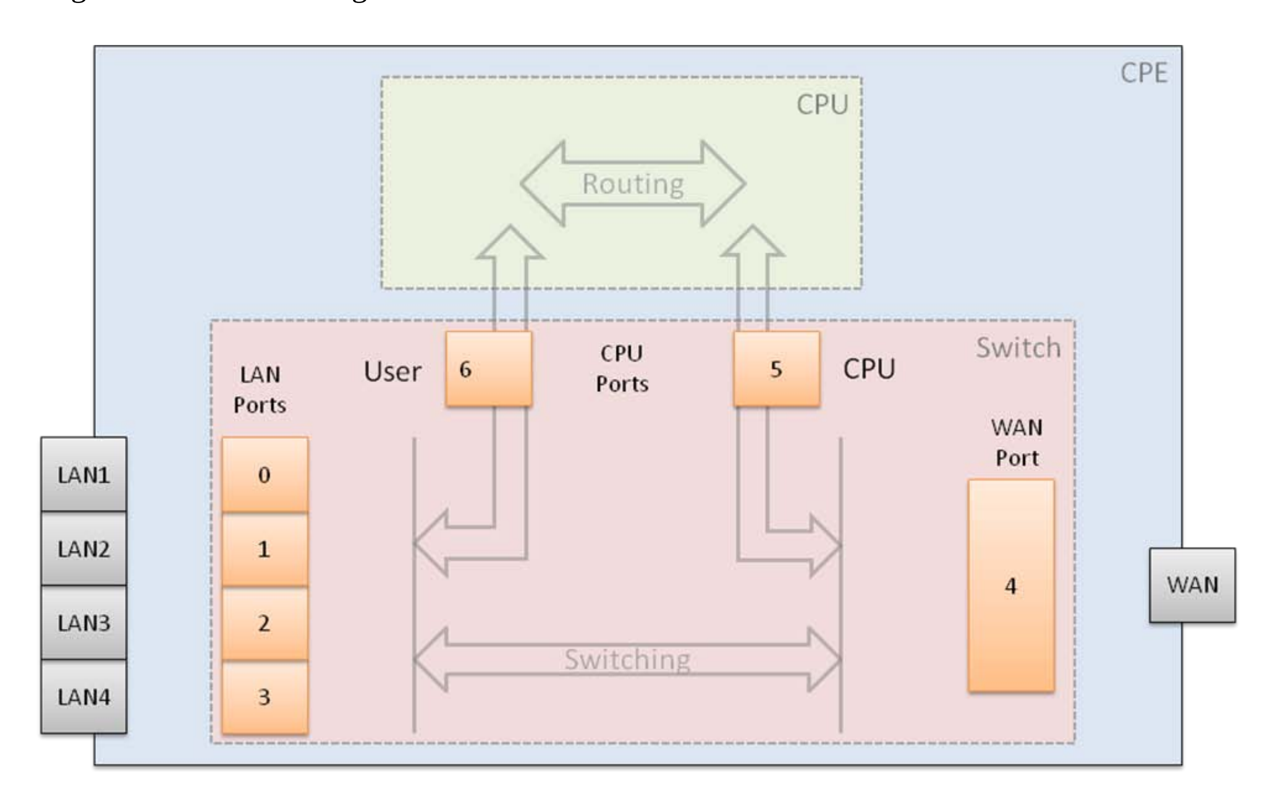


Bild 10: Portzuordnung

Dabei wird zwischen äußeren und inneren Ports unterschieden. Äußere Ports sind auf der LAN-Seite die Ports 0…3 (am Gerät bezeichnet mit LAN1…4!). Auf der WAN-Seite (DSL) ist dies der Port 4 und dieser wird in der GUI-Konfiguration mit „WAN“ bezeichnet. Weiterhin gibt es zwei innere Ports, die für geroutete Pakete verwendet werden (gekennzeichnet mit „User“ und „CPU“). Der mit „User“ bezeichnete Port zeigt Richtung LAN-Seite und der mit „CPU“ bezeichnete Port Richtung WAN-Seite. Beide sind an den inneren Prozessor angeschlossen.

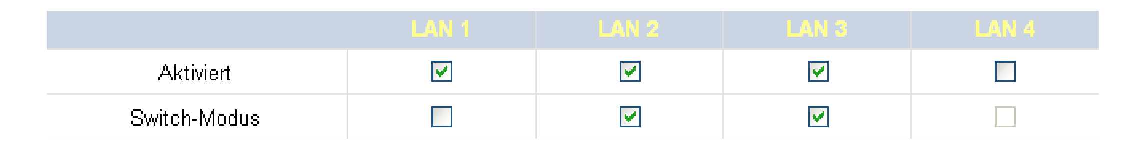
Die umfangreichen Einstellmöglichkeiten werden in den folgenden Kapiteln beschrieben. Ein Beispiel soll bei der Verständlichkeit der Switch-Einstellungen helfen.

3.8.1 Konfiguration LAN-Ports

In diesem Abschnitt können die LAN-Schnittstellen des BIG 10 einzeln aktiviert werden. Es gibt zwei Möglichkeiten, LAN-Ports mit dem WAN zu verbinden:

1. switched: die LAN-Ports sind direkt mit dem WAN-Port verbunden
2. routed: die LAN-Ports sind über die CPU (dem internen Prozessor) mit dem WAN-Port verbunden.

Beispiel: Es stehen die LAN-Ports 1…3 zur Verfügung (LAN4 ist deaktiviert) und LAN2 und LAN3 sind direkt mit der WAN-Schnittstelle verbunden.



	LAN 1	LAN 2	LAN 3	LAN 4
Aktiviert	☑	☑	☑	☐
Switch-Modus	☐	☑	☑	☐

Bild 11: Beispiel Konfiguration LAN-Ports

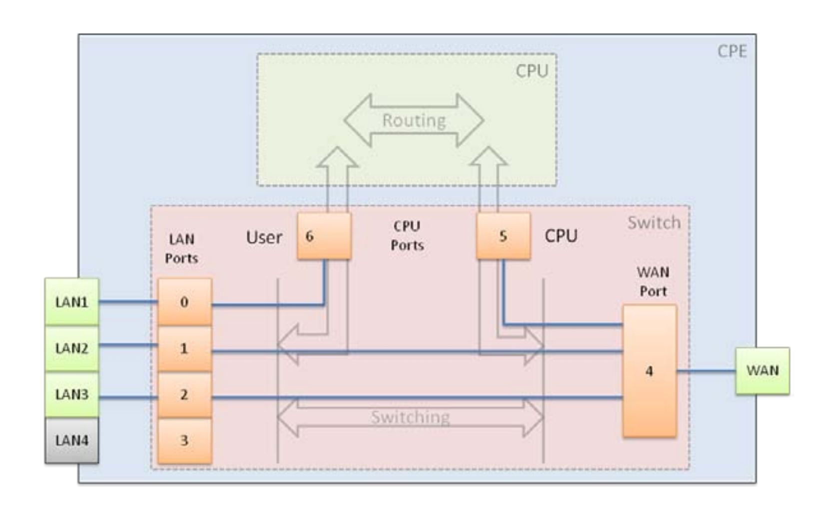


Bild 12: Portzuordnung entsprechend Beispiel Konfiguration

Warnung Mögliche Firewall-Einstellungen sind für den jeweiligen Ethernet-Port im Switch-Modus nicht mehr verfügbar. An diesen Port im Switch-Modus angeschlossene Geräte sind nicht durch die System-Firewall des BIG 10 geschützt!

Zusätzlich können Sie in der LAN-Port-Konfiguration Flow-Control und Auto-Negotiation einstellen.

3.8.2 VLAN-Konfiguration

In diesem Abschnitt können Sie die VLAN-Einstellungen Ihres BIG 10 vornehmen.

Hinweis VLAN können erst konfiguriert werden, wenn mindestens ein LAN-Port mit dem WAN verbunden ist (Switch-Modus, siehe Kapitel 3.8.1). Das Menü „VLAN-Konfiguration" ist auch dann erst sichtbar.



Sie können bis zu 8 VLAN konfigurieren. Vergeben Sie für jedes VLAN die entsprechende VLAN-ID und die VLAN-Priorität.

Warnung Die VLAN-ID 1 wird von vielen Switches nicht unterstützt! Sollten Probleme auftreten, wählen Sie eine andere VLAN-ID (Empfehlung: 2...4094).



Abschließend geben Sie an, welche Ports im Switch-Mode VLAN tagged / untagged angehören.

- „-“ gibt an, dass der Port kein „Member/Mitglied“ des jeweiligen VLANs ist → nur untagged Traffic
- „U“ gibt an, dass der Port „untagged Member/Mitglied“ des jeweiligen VLANs ist → untagged Traffic wird mit VLAN versehen, bei tagged Traffic (VLAN) wird Tag entfernt
- „T“ gibt an, dass der Port „Member/Mitglied“ des jeweiligen VLANs ist → nur Traffic mit dem entsprechenden VLAN
- „S“ gibt an, dass der Port zu jeglichem Traffic ein eingestelltes VLAN-Tag (Service-Tag) anfügt → bei getagged Traffic wird entsprechendes VLAN-Tag entfernt

3.8.3 QoS-Einstellungen

Bestimmte Daten können speziell behandelt werden, um den damit verbundenen Dienst sicherzustellen. Dazu bedient man sich „Quality of Service“ oder einfach QoS-Einstellungen.

QoS-Verbesserungen können auf zwei Wegen erzielt werden. Erstens können über QoS-Regeln Pakete speziell gekennzeichnet werden, um diese bevorzugt zu behandeln. Zweitens können Ports und Queues minimale und maximale Bandbreiten zugewiesen werden. Beide Verfahren werden nacheinander abgearbeitet.

Das folgende Bild zeigt die Abarbeitungsreihenfolge der verschiedenen QoS-Mechanismen:

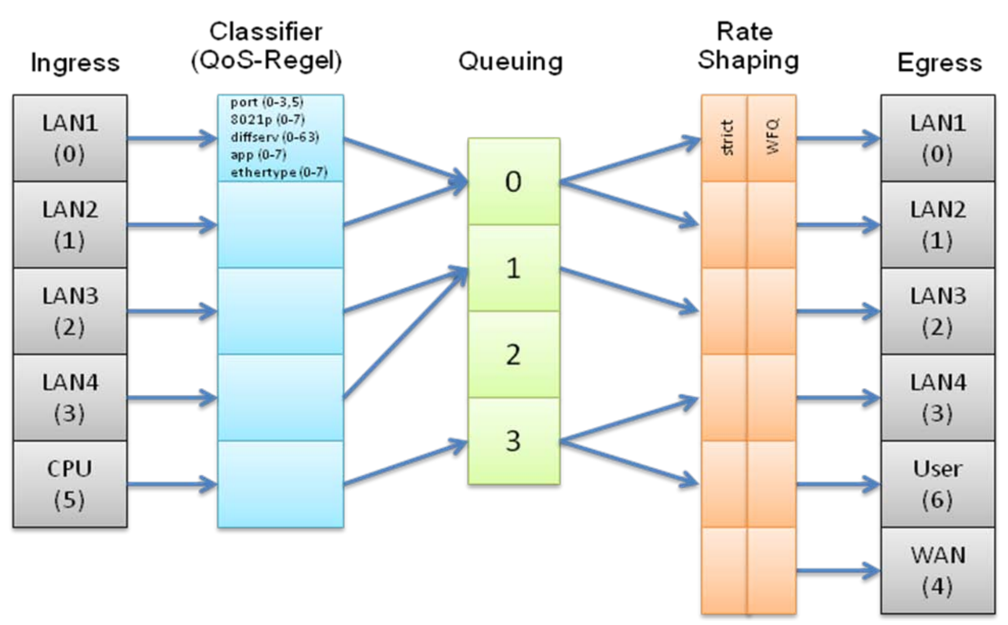


Bild 13: Abarbeitungsreihenfolge der verschiedenen QoS-Mechanismen

Für die Erzielung einer bestmöglichen Dienstgüte (QoS – Quality of Service) besitzt das Gerät vier interne Warteschlangen (Queues), in die Pakete unterschiedlicher Priorität eingeordnet werden können. Diese haben voreingestellte, nicht änderbare Prioritäten:

Queue	Priorität
0	gering
1	normal
2	hoch
3	höchste

In diese Queues können die QoS-Regeln aller Switch-Ports eingeordnet werden, die im Folgenden beschrieben werden.

3.8.4 QoS-Regeln

In diesem Abschnitt werden die Regeln zur Klassifizierung von eingehendem (Ingress) Datenverkehr definiert. Gleichzeitig erfolgt eine direkte Zuordnung in eine der 4 Priority-Queues (höchste, hoch, normal, gering).

Hinweis



Um die QoS-Regeln an den LAN-Ports anwenden zu können, müssen diese im Switch-Modus konfiguriert sein. Siehe dazu auch Kapitel 3.8.1.

Rx-Port
Auf dieser Seite kann eingestellt werden, wie eingehender Datenverkehr am jeweiligen Rx-Port (Empfangsseite der LAN-/WAN-Ports) klassifiziert wird. D.h., es erfolgt eine Zuordnung in eine der 4 Priority-Queues. Zum Aktivieren dieser Regel muss diese im Bedarfsfall für den jeweiligen Rx-Port im Abschnitt „QoS-Einstellungen“ selektiert werden.

802.1p
Auf dieser Seite kann eingestellt werden, wie eingehender Datenverkehr anhand der VLAN-Priorität (IEEE 802.1p) klassifiziert wird. Zum Aktivieren dieser Regel muss diese im Bedarfsfall für den jeweiligen LAN-Port im Abschnitt „QoS-Einstellungen“ selektiert werden.

DiffServ
Auf dieser Seite kann eingestellt werden, wie eingehender Datenverkehr anhand des DSCP (DiffServ Code Point) klassifiziert wird. Zum Aktivieren dieser Regel muss diese im Bedarfsfall für den jeweiligen Port im Abschnitt „QoS-Einstellungen“ selektiert werden.



Application
Auf dieser Seite kann eingestellt werden, wie eingehender Datenverkehr, welcher einer bestimmten Anwendung (Applikation) zugeordnet werden kann, klassifiziert wird. Die Zuordnung des Datenverkehrs zu einer Anwendung kann durch Auswertung der Quell- bzw. Ziel-Portnummer im UDP/TCP-Paket-Header erfolgen. Hierbei besteht die Möglichkeit, den Quell- oder Ziel-Port bzw. beide gleichzeitig als Kriterium zu verwenden. Ebenfalls kann ein Portbereich angegeben werden. Dieser kann sich zwischen 1 und 255 ausgehend vom Anfangsport erstrecken. Zum Aktivieren dieser Regel muss diese im Bedarfsfall für den jeweiligen Port im Abschnitt „QoS-Einstellungen“ selektiert werden.

EtherType
Auf dieser Seite kann eingestellt werden, wie eingehender Datenverkehr anhand des EtherType-Feldes im Ethernet-Frame-Header klassifiziert wird. Zum Aktivieren dieser Regel muss diese im Bedarfsfall für den jeweiligen Port im Abschnitt „QoS-Einstellungen“ selektiert werden.

3.8.5 QoS-Bandbreite

Auf dieser Seite kann die Bandbreitenbegrenzung auf Basis der vier Prioritätsqueues eingestellt werden. Dazu gehen Sie wie folgt vor:

1. Geben Sie die eingehende (Ingress) Bandbreite in kbit/s ein.
2. Mit dem Parameter „WFQ-Typ“ lässt sich einstellen, wie die Werte zu den Parametern zu interpretieren sind, sprich: stellen die Werte konkrete Bandbreite-Einstellungen in kbit/s (max Mode) oder eine Gewichtung (ratio Mode) dar. Im „ratio Mode“ wird die gesamte verfügbare Bandbreite auf die 4 Queues gemäß deren Gewichtung aufgeteilt – im „max Mode“ hingegen (maximal) bis zum jeweils eingestellten Wert in kbit/s.
3. Geben Sie entsprechend der Bandbreitenaufteilung die Werte für eine garantierte Bandbreite (SPC – strict priority queuing) für jede Queue ein. Diese entspricht einer auf einen Wert eingestellten Bandbreite, wenn diese zur Verfügung steht.
   und / oder
4. Geben Sie entsprechend der Bandbreitenaufteilung die Werte für eine gewichtete Bandbreite (WFQ – weighted fair queuing) für jede Queue ein. Der WFQ-Wert jeder einzelnen Queue darf dabei nicht größer sein, als das 3-fache der für WFQ zur Verfügung stehenden Bandbreite pro Queue (Bsp.: gesamt stehen 40 Mbit/s für WFQ zur Verfügung, d.h. pro Queue 10 Mbit/s; eingestellt werden kann jetzt pro Queue 30 Mbit/s).

Wiederholen Sie dies für jeden der gewünschten Ports.
Die Gesamtbandbreite ist dabei immer die Summe aus garantierter (SPC) und gewichteter (WFQ) Bandbreite.

Hinweis Die Bandbreite kann in Schritten von 64 kbit/s eingestellt werden.



Beispiel: Das folgende Beispiel zeigt umfangreiche QoS-Einstellungen.

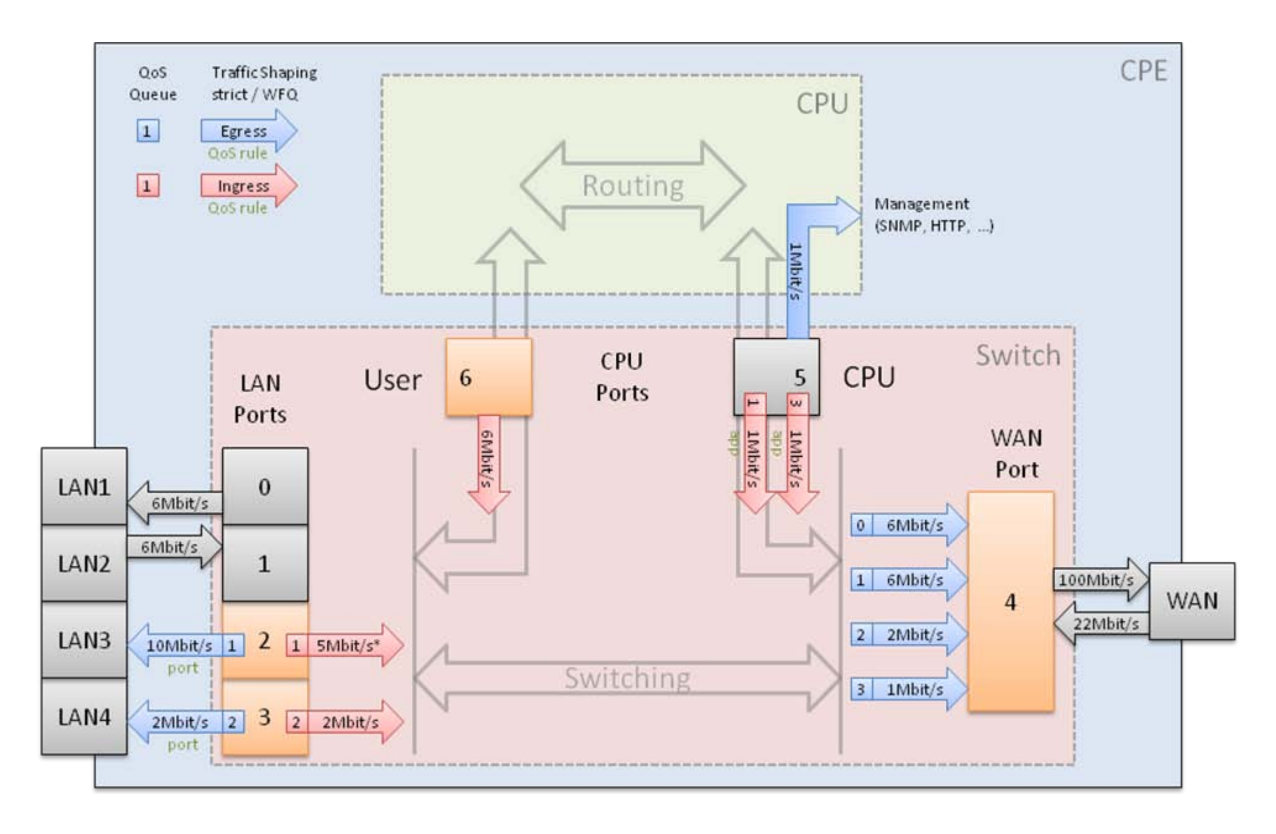


Bild 14: Beispiel QoS-Einstellungen

Das Gerät verfügt über eine Gesamtbandbreite der WAN-Seite (SHDSL) von 22 Mbit/s. Die physischen LAN-Ports 1 und 2 sind geroutet über die internen CPU-Ports (User, CPU). Die LAN-Ports 3 und 4 sind direkt mit dem WAN-Port verbunden (switched).

Hinweis Bitte beachten Sie, dass die Switch-Ports immer eine Bandbreite von 100 Mbit/s besitzen. Daher ist auch die Geschwindigkeit Richtung WAN (zum SHDSL) 100 Mbit/s und wird erst durch die SHDSL-Bandbreite begrenzt.

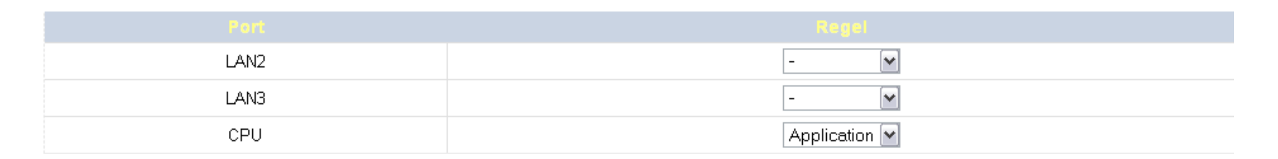


Der interne Datenverkehr des Managements bekommt eine feste Bandbreite von 1 Mbit/s zugewiesen. Dieser ausgehende Verkehr wird in die Queue 3 mit der höchsten Prioritätsklasse eingeordnet über eine „Application“-QoS-Regel. Hier ist es exemplarisch Verkehr über den TCP-Port 8080 (http zugewiesen).
An die LAN-Ports 1 und 2 angeschlossene Geräte können für eine spezielle Anwendung (z.B. ERP-Software, VPN, etc.) eine garantierte Bandbreite von 1 Mbit/s zugewiesen bekommen, sofern diese Anwendung den TCP-Port 30000 verwendet. Die Daten sind in die Queue 1 (Priorität normal) eingeordnet.
Die LAN-Ports 1 und 2 sind darüber hinaus auf eine Datenrate (up-/downstream) von 6 Mbit/s eingestellt, ohne jegliche Priorisierung des Datenverkehrs (z.B. normale Internet- oder E-Mail-Daten).
LAN-Port 3 bekommt 10 Mbit/s downstream und 5 Mbit/s upstream zugewiesen mit der Priorität 1 (normal, Queue 1). Eine Zuweisung der Bandbreite am Switchport 2 ist nur notwendig,



wenn sehr hoher UDP-Datenverkehr zu erwarten ist. Ansonsten ist die Begrenzung der Queue am WAN-Port ausreichend.
LAN-Port 4 bekommt (z.B. für eine VoIP-TK-Anlage) 2 Mbit/s symmetrisch zugewiesen mit der hohen Prioritätsklasse, damit Queue 2.
Für das beschriebene Beispiel sind folgende Einstellungen im BIG 10 vorzunehmen:

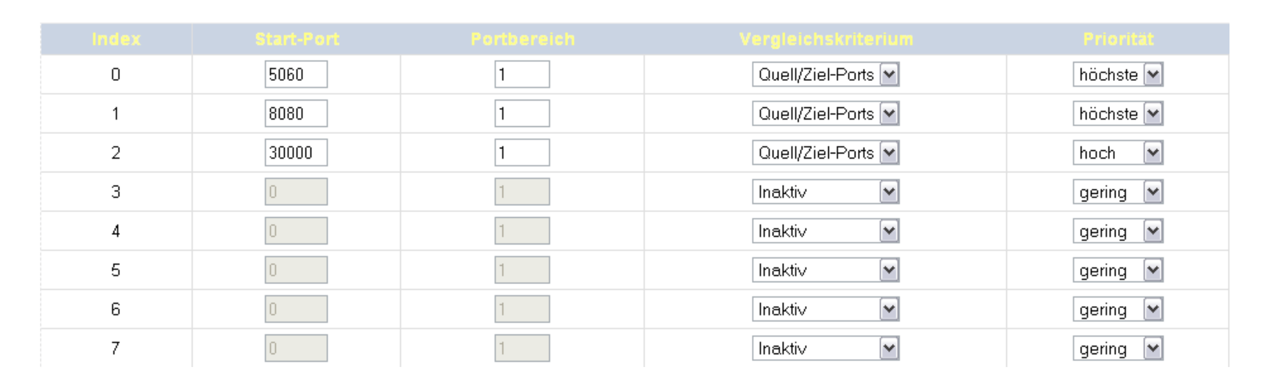
Unter QoS-Einstellungen:
Die internen Ports LAN2/3 (physikalische LAN-Ports 3/4) sind direkt mit dem WAN-Port verbunden.



Port	Regel
LAN2	-
LAN3	-
CPU	Application

Bild 15: Beispiel QoS-Einstellungen

Unter QoS-Regeln / Application:



Index	Start-Port	Portbereich	Vergleichskriterium	Priorität
0	5060	1	Quell/Ziel-Ports	höchste
1	8080	1	Quell/Ziel-Ports	höchste
2	30000	1	Quell/Ziel-Ports	hoch
3	0	1	Inaktiv	gering
4	0	1	Inaktiv	gering
5	0	1	Inaktiv	gering
6	0	1	Inaktiv	gering
7	0	1	Inaktiv	gering

Bild 16: Beispiel QoS-Regeln / Application

Unter QoS-Bandbreite:



			SPQ (Garantierte kbit/s)				WFQ (Max. kbit/s)/Gewichtung (Ratio)			
Port	Ingress [kbit/s]	WFQ Typ	Q3	Q2	Q1	Q0	Q3	Q2	Q1	Q0
LAN2	102400	ratio Mode	102400	102400	102400	102400	102400	102400	102400	102400
LAN3	102400	ratio Mode	102400	102400	102400	102400	102400	102400	102400	102400
WAN	102400	ratio Mode	102400	102400	102400	102400	102400	102400	102400	102400
CPU	102400	ratio Mode	102400	102400	102400	102400	102400	102400	102400	102400
USER	102400	ratio Mode	102400	102400	102400	102400	102400	102400	102400	102400

Bild 17: Beispiel QoS-Bandbreite

3.8.6 Smart Discard

Der BIG 10 unterstützt ein innovatives Verfahren, um Pakete früher in Abhängigkeit ihrer Priorität zu verwerfen, um Ressourcenengpässe der QoS-Queues durch Pakete mit niedriger Priorität zu verhindern.
Der „Smart Discard“ Mechanismus kann für jede der vier Queues separat konfiguriert werden. Die Modi haben dabei folgende Funktion:

Modus	bei Auslastung	verworfene Pakete
Mode 0	> 0%	0%
Mode 1	> 0% > 75%	0% 25%
Mode 2	> 0% > 50% > 75%	0% 50% 75%
Mode 3	> 0% > 25% > 50%	0% 25% 50%

3.8.7 Port-Sicherheit

Die in diesem Abschnitt konfigurierbare Port-Sicherheit erlaubt es, dass nur Ethernet-Frames mit dynamisch angelernten MAC-Adressen oder solche mit statisch Eingetragenen durch den jeweiligen Ethernet-Port des BIG 10 hindurch gelassen werden.

Hinweis: Die Port-Sicherheit ist an den einzelnen Ports deaktiviert, wenn jeweils der MAC-Adress-Filter nicht aktiv ist und bei MAC-Adress-Limitierung der Wert "0" selektiert ist.



3.8.8 Statistiken

Hier können Sie sich Statistik-Informationen für jeden Switch-Port anzeigen lassen.

3.8.9 Monitoring

Auf dieser Seite können Sie konfigurieren, inwiefern eingehender und/oder ausgehender Datenverkehr eines beliebigen LAN-Ports bzw. WAN-Ports an einem weiteren LAN-Port gespiegelt werden soll.
Wählen Sie einen Zielport aus, zu dem die Daten gespiegelt werden sollen und einen Quell-Port, von dem die Daten stammen.



3.9 SHDSL

Dieser Abschnitt zeigt den Status und die Konfiguration der SHDSL-Schnittstellen des BIG 10.

3.9.1 Config

Auf dieser Seite können ausgewählte SHDSL-Parameter konfiguriert werden.

Operating Mode
Der Betriebs- (oder Operating-) Mode verfügt über verschiedene Einstellungen. Die Konfiguration ist möglich in den Modi RT ("Remote Terminal" bzw. CPE) oder COT ("Central Office Terminal").

EFM G.hs Mode
ITU G.hs gemäß ITU-T G.994.1 und IEEE802.3ah

PMMS Mode (Line Probing)
Line Probing gemäß ITU-T G.991.2 (2004)

PMMS Target Margin
Gewünschter Signal-Rausch-Abstand für den PMMS-Mode

3.9.2 Status

Der Status aller SHDSL-Linien wird hier angezeigt. Sie können die Anzeige entweder manuell aktualisieren („Aktualisieren"-Button) oder automatisch durch Drücken des „Zyklisch Aktualisieren"-Buttons.

Linestatus

Down (Idle) / Down (Ready)	Link down / Verbindungsausfall
PCS Sync	Bonding-Gruppe eingerichtet
G.hs Line Probing	Aushandeln der Leitungsparameter
G.hs Transfer	Aushandeln der Leitungsparameter
Data Mode	Leitung ist im Datenübertragungsmodus

Datenrate
Folgende Datenraten (in kbit/s) lassen sich mit dem BIG 10 in Abhängigkeit der Einstellungen der zentralen Seite (CO) erzielen:

Annex	**Modulation**	**1-Paar bzw. 2-Draht**	**2-Paar bzw. 4-Draht**	**3-Paar bzw. 6-Draht**	**4-Paar bzw. 8-Draht**
Annex A/B	TC-PAM-16	192… 2304	384… 4608	576… 6912	768… 9216
Annex AF/BG	TC-PAM-16	192… 3840	384… 7680	576…11520	768…15360
	TC-PAM-32	768… 5696	1536…11392	2304…17088	3072…22784

Loop Attenuation (dB)
Gemessener Leitungsdämpfungswert in dB [je länger, desto größer]

SNR (dB)
Der Signal-Rausch-Abstand („SNR - signal noise ratio“) ist ein Index der Qualität der Leitungsverbindung. Je größer der SNR ist, umso besser ist die Leitungsqualität. Der Bereich des SNR geht von -10 dB bis 21 dB.

3.9.3 Performance

Diese Seite zeigt aktuelle Performance-Daten aller SHDSL-Linien an. Angezeigt werden:

Uhrzeit
Anzeige der Uhrzeit nach Aktivieren der NTP-Funktion bzw. Anzeige der abgelaufenen Zeit (24 h) nach Aktivierung der SHDSL-Leitung

TMP (total measurement period)
Gesamte Dauer (Zeitintervall) der Zählung der Leistungsdaten; wird nach 15 Minuten = 900 Sekunden zurückgesetzt

ES (errored seconds)
Anzahl der Sekunden, in denen Fehler aufgetreten sind

SES (severe errored seconds)
Anzahl der Sekunden, in denen schwere Fehler aufgetreten sind

CRC6 (cyclic redundancy check)
Anzahl der CRC6-Fehler

LOSW (los of sync word)
Anzahl der LOSW-Fehler

UAS (unavailable seconds)
Anzahl der Sekunden, in denen keine Übertragung möglich war

3.9.4 Performance History

Zur Auswahl der SHDSL-Linie klicken Sie auf die entsprechende Zahl oberhalb der Tabelle. Die Performancy History zeigt alle Fehler von den 15-Minuten-Intervallen innerhalb eines Tages (24 Stunden) an.



4 Technische Daten

WAN-Schnittstelle (SHDSL)

Norm	ITU-T G.991.2 G.SHDSL.bis; 2/4 SHDSL-Leitungspaare
Bandbreite	hohe symmetrische Bandbreite (bis zu 22 Mbit/s) durch Unterstützung von EFM-Bonding (IEEE 802.3-2004) und ATM-Bonding (Unterstützung des M-Pair-Modus)
Steckverbinder	1 × RJ45

ATM

- ATM-Layer nach I.361
- AAL5 nach I.363.5
- VPI/VCI Range konfigurierbar
- Unterstützung von OAM F4/F5, AIS, RDI, und loopback

LAN-Schnittstelle (Ethernet)

Norm	Standard-Ethernet-Protokoll IEEE 802.3, IEEE 802.1q, 802.1d, native Multicast,
VLAN	VLAN double tagging as per IEEE 803.2ac VLAN-Unterstützung für Management- und Nutzerdaten DSCP remarking
Ethernet-Merkmale	10/100 Base-T, MDI/MDIX-Autosensing, TCP/IP
Bridge-Funktionen	Transparentes Layer 2 Bridging
max. Frame-Größe	1536 Byte (Switch Mode) 1518 Byte (Router Mode, Restricted Mode)
Steckverbinder	4 × RJ45

Router-Funktionen

- TCP/IP v4
- NAT
  - virtuelle Server
  - Portmapping
  - virtuelle DMZ
- DHCP-Client/Server
- PPPoE
- statische IP
- Firewall
- DynDNS

Quality of Service

- Strict Priority (SPQ) & Weighted Fair Queuing (WFQ)
- Definition von Serviceklassen (CoS)
  - Port-based
  - 802-1p
  - DSCP
  - Application based (TCP port)
  - Ethertype
- Bandbreiten-Management (shaping), Bandbreiten-Begrenzung (limiting)

OAM

- Dying-Gasp
- NTP
- MAC-Adress-Filter
- statistische Übertragungsdaten und Historie

WLAN-Schnittstelle (nur Art.-Nr. 900220)

Access-Point	nach IEEE802.11b/g
802.11g Datenrate	54, 48, 36, 24, 12, 9, 9 Mbit/s
802.11b Datenrate	11, 5.5, 2, 1 Mbit/s
Sicherheit	64- / 128-bit WEB; WPA-PSK, WPA2-PSK, WPA, WPA2
Übertragungsleistung	bis zu 100 mW
Antenne	extern

Management und Konfiguration

Konfiguration	über integrierte Web-GUI (lokal); SNMP v2 / v3; DHCP / TFTP (remote mittels Konfigurationsdatei)
Sicherheit	Passwortschutz der Konfiguration

Stromversorgung Steckernetzteil

Betriebsspannungsbereich	100 V … 240 V ∼
Frequenzbereich	50 Hz … 60 Hz
Stromaufnahme	≤ 0,5 A
Stecker	Eurostecker

Stromversorgung BIG 10

Nennspannung	12 V ⎓
Stromaufnahme	< 1,2 A

Gehäuse

Ausführungsvariante	Kunststoffgehäuse mit integrierten Anzeigeelementen und physikalischen Schnittstellen
Anzeigeelemente	4 (5) LEDs zur Statusanzeige
Gehäuseabmessungen	240,4 × 160,4 × 48,2 mm^3 (B × T × H)
Gehäusefarbe	signalweiß (RAL 9003), tiefschwarz (RAL 9005)
Gewicht	1,0 kg

Umgebungsbedingungen (gemäß ETS 300 019)

Lagerung und Transport	Lufttemperatur: -40°C ... +70°C Luftfeuchtigkeit: 0% ... 85% (nicht kondensierend)
Betrieb	Lufttemperatur: 0°C ... +45°C Luftfeuchtigkeit: 10% ... 85% (nicht kondensierend)

Standards, Zertifikate

EMV	ETSI EN 300 386, EN 55022 Klasse B, ETSI ES 201 468, ITU-T K.21
Sicherheit	EN 60950-1



5 Wichtige Hinweise

5.1 Herstellererklärung

Der Hersteller erklärt, dass das ELCONnect next BIG 10 Router für die Übertragung von Informationsdaten vorgesehen ist und bei bestimmungsgemäßer Verwendung den geltenden Normen bezüglich Sicherheit und elektromagnetischer Verträglichkeit entspricht.

5.2 Gewährleistung

Die vorliegende Dokumentation von ELCON Systemtechnik GmbH basiert auf dem aktuellen Stand der Technik. Trotz aller Sorgfalt lassen sich Fehler und technische Ungenauigkeiten nicht immer vermeiden. Als Ergebnis des schnellen technischen Fortschrittes behält sich ELCON das Recht vor, technische Änderungen und Entwicklungen ohne vorherige Anzeige durchzuführen.
Aus diesem Grunde gibt ELCON keine Garantie für den Inhalt des vorliegenden Dokumentes.

Außerdem ist ELCON nicht verantwortlich für den Verlust oder die inkorrekte Nutzung von Informationen und Daten, welche aus dem Gebrauch des Dokumentes resultieren können. Weiterhin ist ELCON nicht verantwortlich für Zerstörungen oder indirekte Zerstörung (dies beinhaltet auch finanzielle Verluste, verzögerte Geschäftstransaktionen oder Geschäftsabbruch sowie ähnliche Konsequenzen), welche durch falsche Benutzung der Geräte entstehen.

Die vorliegende Dokumentation ist gestaltet, um die Funktionsweise des ELCONnect next BIG 10 Router zu erläutern. Es erklärt die Installation und den Gebrauch des Gerätes sowie gegebenenfalls notwendiger Zusatzkomponenten, Treiber und Softwaretools. Zusätzliche Detailangaben, welche gezielt auf kundenspezifische Lösungen eingehen, sind dem jeweiligen Benutzerhandbuch zu entnehmen.

Für weitere Informationen zum Betrieb peripherer Geräte und Anlagen, insbesondere zur Installation von Computerhardware sowie den netzseitig verfügbaren Zugangstechnologien informieren Sie sich bei Ihrem Telekommunikationsnetzbetreiber oder Internet Service Provider beziehungsweise in den jeweiligen Nutzerhandbüchern.
Es ist möglich, dass in der Dokumentation beschriebene Leistungsmerkmale nicht im konkreten Anwendungsfall genutzt werden können.

5.3 Rechte und Warenzeichen

Mit Bezug auf die in der Dokumentation enthaltenen Daten garantiert ELCON nicht für die Nichtexistenz von industriellen Eigentumsrechten (Warenzeichen, Patente, Gebrauchsmuster, etc.). Warenzeichen, Markennamen, Firmen- und Produktnamen im generellen Gebrauch sind Subjekt zum jeweiligen Warenzeichen, Patent, Gebrauchsmuster und registrierten Designrechten.

Die vorliegenden Informationen dürfen weder teilweise noch im Ganzen kopiert, übersetzt, nachgedruckt oder in irgendeiner anderen Weise transferiert werden.

Der Bezug von Software und Geräten unterliegt den Allgemeinen Geschäftsbedingungen sowie den Lizenzbedingungen der ELCON Systemtechnik GmbH.

ENGLISH

1 Technical description of the BIG 10

1.1 Scope of application

Business customers today need a modern and efficient communication infrastructure, so they require extremely flexible, high-performance transmission systems and terminal equipment. Special attention is hereby paid to meet the demand for highly available, symmetrical broadband services with conventional Service Level Agreement (SLA), as well as the requirements with respect to bandwidth management, separation of the individual voice and data services, and the guaranteed availability of certain services (e.g. VoIP) using efficient prioritization algorithms.

The products from the Business IP Gateway (BIG 10) series are specially designed for business customers.

The BIG 10 products are optimized for data applications, such as the transmission of Internet data, the connection of external locations to a central office by setting up virtual local area networks (VLAN), or the transmission of voice and video information in real time for VoIP and video conferences. It provides a variety of functions for efficient band-width management and the prioritization of services and interfaces. The unit can also be used to feed Mini-DSLAM's in remote outdoor locations that are not linked over an optical fiber connection. The BIG 10 can be used as stand-alone device for transparent WAN-LAN bridging on layer 2 for individual PC's, too, but also for downstream IAD's, routers and DSLAMs.

The BIG 10 router offers a managed switch and router, thus providing an ideally suited device to meet different customer requirements.

Data transmission to the IP backbone runs over max. 4 SHDSL lines, which can provide data rates of up to 5.7 Mbps per each line pair, using the eSHDSL transmission method. The special EFM-Bonding allows increasing the total capacity of the business customer access to even 22 Mbps. Bandwidth expansions can be very easily realized by adding further SHDSL lines to the bonding group, so that the customer's demand for higher bandwidths will be met without delay.

The high availability of the business customer access and the individual services provided along can be guaranteed. The high requirements with respect to continuous availability of the business access are perfectly met with the optional Dying Gasp function, which signals local power failures to the system administrator, enabling the network operator to adequately react in good time.

Local and remote configuration as well as management is realized by the implemented Local Craft Terminal (LCT) resp. the implemented SNMP-protocol which guarantees that the efforts for OAM are kept to a minimum. Remote management of 3rd party SHDSL DSLAMs is realized through the implemented EOC-protocol, which can be accordingly adapted in case of need.



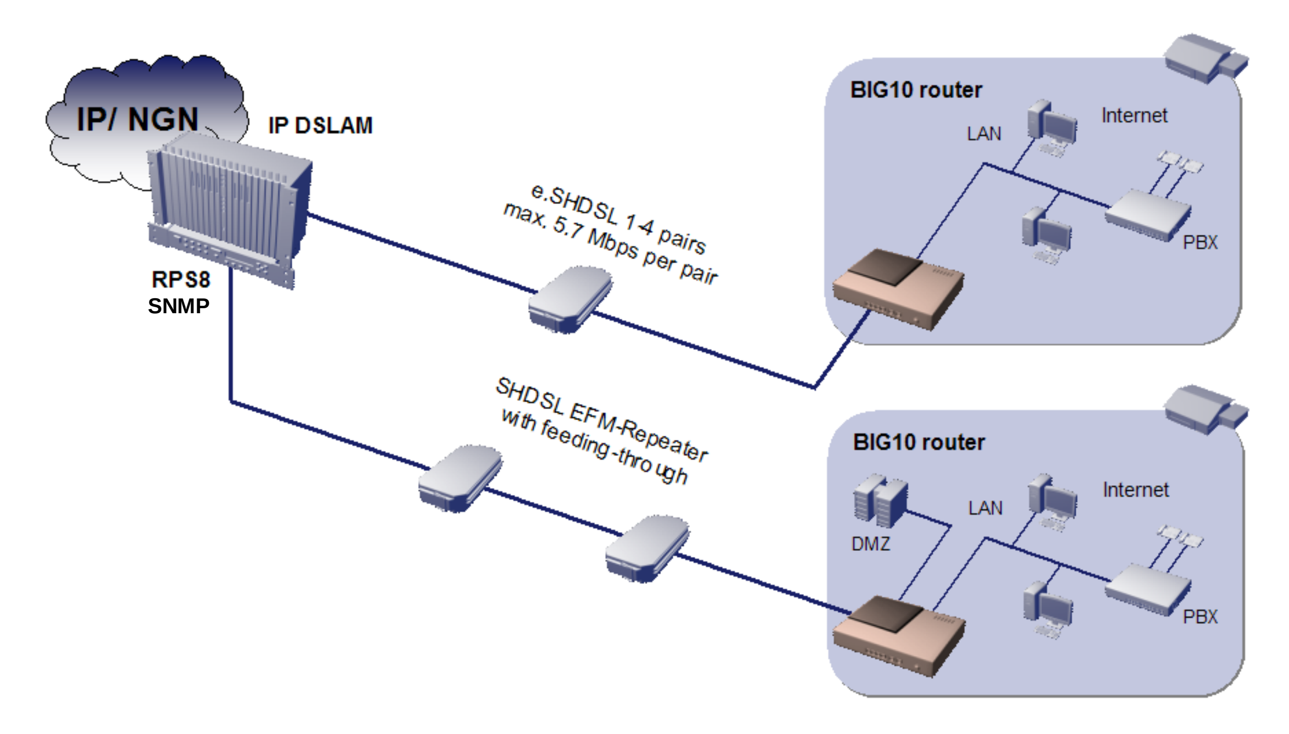


Figure 1: Basic application scenario

1.2 General characteristics

- symmetrical data transfer at max. 22 Mbps via standard copper wire pairs
- 2/4 × SHDSL EFM with eSHDSL and EFM-Bonding support
- range extension using up to 4 repeaters or flexible adaptation of the SHDSL bit rate
- calibration of the copper twin wire and specific setup of target noise margins via Line Probing (PMMS)
- customer interfaces
  - 4 × Ethernet
  - WLAN 802.11b/g (only order no. 900220)
- switch and router support, support of transparent layer 2 bridging and routing
- operation as NT with third-party DSLAM's
- support of VLAN Tagging for the separation of voice and data services
- traffic shaping and prioritization support for guaranteed high QoS
- support of IPSec pass-through
- local and remote management via GUI; integration in 3rd-party NMS via SNMP
- SNMP v1/v2/v3 support
- local power supply

2 Installation

2.1 Hardware requirements / Minimum system requirements for installation of the BIG 10

- Power socket providing nominal voltage range 100 V … 240 V ~ / 50 Hz … 60 Hz
- Laptop or PC running on OS Windows® 98 SE, ME, 2000, XP; MAC; Linux and full-duplex network interface card (interface: 10/100Base-T); CPU: Pentium II®, 500 MHz or higher
- if necessary: diverse tools for wall-mounting (water-level, pencil, drilling machine, drill Ø 6 mm, screwdriver)

2.2 Scope of delivery

- 1 BIG 10 Router with external plug-in power supply unit 12 V ⎓, 1.2 A
  - Order no. 900216: BIG 1022 (2-port SHDSL)
  - Order no. 900217: BIG 1024 (4-port SHDSL)
  - Order no. 900220: BIG 1044 (4-port SHDSL / WLAN)
- 1 plug-in power supply unit (12 V ⎓, 1.2 A)
- 1 Ethernet cable, yellow, 3 m
- 1 drilling template
- 1 toolkit bag (2 dowels, 2 screws)
- 1 operating manual

2.3 Selecting the place of installation / Fixing the device

The BIG 10 has been designed for in-house use in closed rooms. It may be operated as desk-top unit or fixed to the wall. The BIG 10 should be placed nearby the DSL cable and next to a mains socket. Since the BIG 10 is determined for continuous operation, it has no mains switch. For disconnection from the electricity grid, just remove the plug-in power supply unit. So the wall power supply should always be easily accessible.

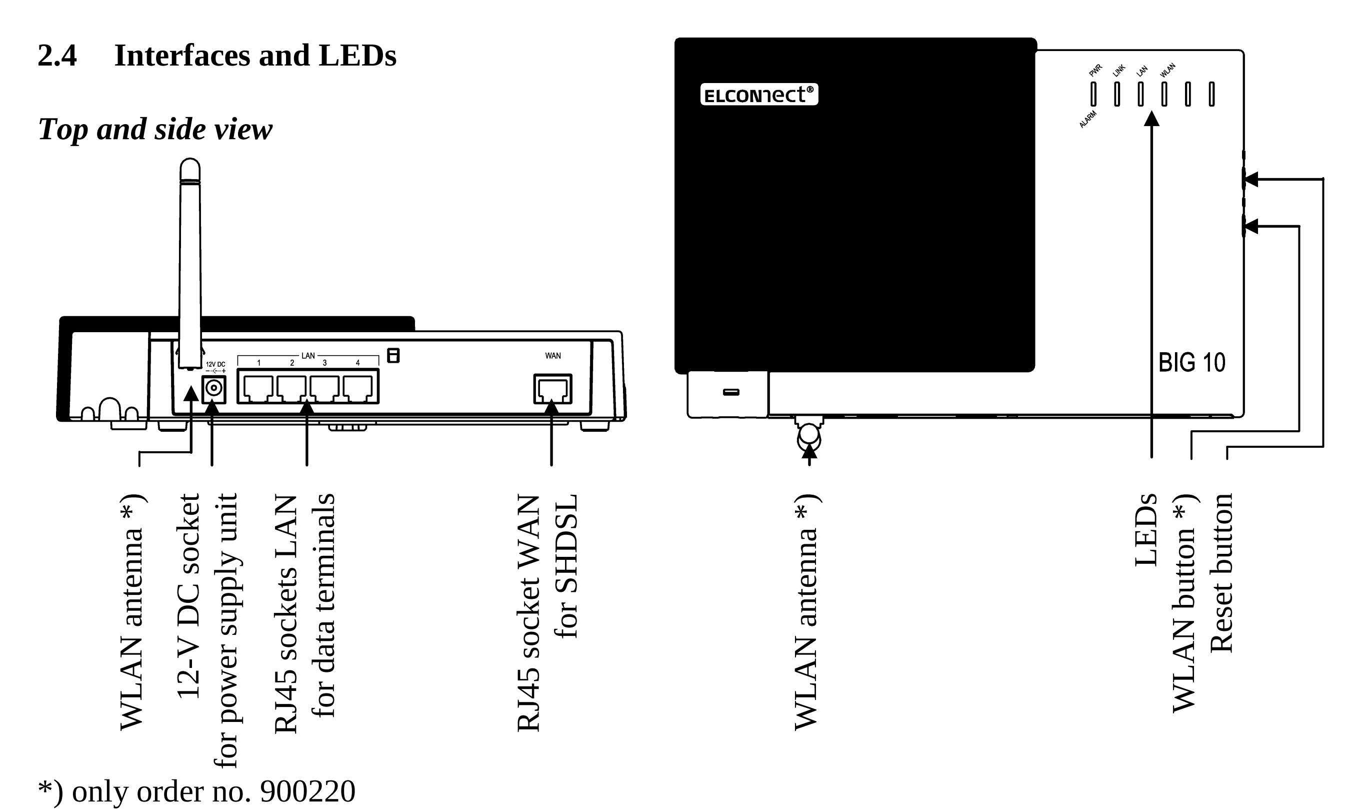
Prior to wall mounting, make sure that there are no concealed supply lines (power, water, gas, telephone, coaxial or fiber cable) at the intended installation place. During operation, the BIG 10 is markedly warming up, but this operating temperature is not dangerous at all. However, to provide for unimpeded heat dissipation, the BIG 10 must not be installed into a fully closed casing, lacking of a sufficiently dimensioned breather hole. For the same reason the device shall also be protected from intensive heating, caused e.g. by heating appliances or direct sun radiation. Further, do not expose the modem to a very humid or dusty environment.

The mounting instructions can be found on the drilling template.



2.4 Interfaces and LEDs

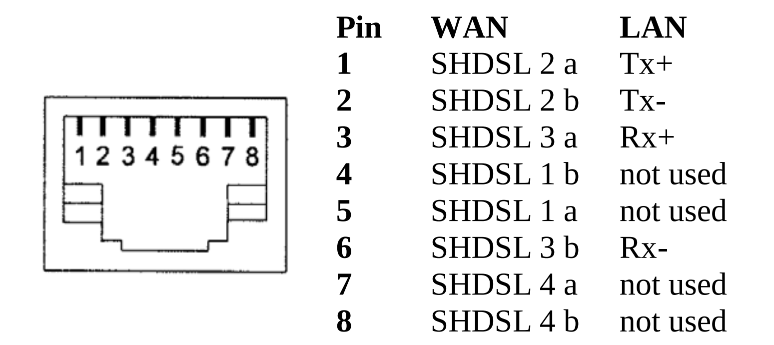
Top and side view



*) only order no. 900220

Figure 2: Top and side view of the BIG 10

Pin assignment of the RJ45 sockets (WAN, LAN)



Pin	**WAN**	**LAN**
1	SHDSL 2 a	Tx+
2	SHDSL 2 b	Tx-
3	SHDSL 3 a	Rx+
4	SHDSL 1 b	not used
5	SHDSL 1 a	not used
6	SHDSL 3 b	Rx-
7	SHDSL 4 a	not used
8	SHDSL 4 b	not used

Figure 3: Pin assignment of the RJ45 sockets

LED signalling

The modem has 4 (5) LEDs which signal the data transfer activities.

LED	**Colour**	**Status**	**Meaning**
PWR Status of power supply	yellow	OFF	no mains voltage applied
		ON	mains voltage applied
ALARM Status of alarm	red	OFF	no relevant alarm message received
		blinking	device-initialization after switching-on, until ready-state
		ON	relevant alarm message received or after reset until ready-state

LED	Colour	Status	Meaning
LINK Status of SHDSL	green	OFF	WAN link not established
		flashing	Data-transfer over minimum one SHDSL
		ON	all PCS member sync; WAN link established
	yellow	OFF	State WAN init done; all links down; all PCS member sync; state without any interference
		ON	fastest link PCS sync, still not all members sync; state with any interference
		flashing (slow)	link-ID (1…4) fastest link G.hs-transfer (up to 4 ON-pulses within 2 seconds)
		flashing (inverse)	fastest link line probing
		blinking at 1 Hz	fastest link training; „SHDSL Training“ status
		blinking at 2 Hz	fastest link data mode; „Line Probing“ status
		blinking at 4 Hz	(re-)init running; „G.hs“ status
LAN Status of LAN	green	OFF	LAN-port not established
		flashing (inverse)	data-transfer over minimum one LAN-port
		ON	Link established to at least one LAN port
	yellow	OFF	state without any interference
		ON	state with any interference
WLAN (only order no. 900220) Status WLAN	blue	OFF	WLAN deactivated
		flashing (inverse)	data transfer via WLAN
		ON	WLAN activated
	yellow	OFF	state without any interference
		blinking	after switching-on, until ready-state of WLAN access point
		ON	initialization / state with any interference

2.5 Cable connection

1. Connect the WAN-interface of the BIG 10 with the access port of your network operator, using a UTP (Unshielded Twisted Pair) CAT5 cable or better, to ensure optimal transmission parameters. The cable contact assignment at the socket can be requested from your network provider.
2. Link the BIG 10 with the network interface card of the PC. For this, use an Ethernet cable and connect it to one of the „LAN“-marked RJ45-sockets on the BIG 10 and to the RJ45-socket of the network interface card (see the related instructions).
3. Finally use the enclosed plug-in power supply module to connect the socket „12V DC“ of the BIG 10 to the electricity network. Do not use any other power supply module than the one included in delivery. The use of other power supply units will result in the loss of the CE conformance and exclude any warranty claims.



2.6 Putting into operation

After application of the supply voltage and performed self-configuration the BIG 10 is ready for work. The complete line of the provider network to the BIG 10 will be put into operation by your operator. It has a preset configuration or makes the required settings automatically by auto-configuration.
Prerequisite for proper operation of your data link via the BIG 10 is the correct installation of the network interface card to your PCs. Detailed information on this should be received in the documentation provided by the card manufacturer. Further questions about configuration of your PC should be addressed to your Service Provider.

2.7 Restart and Factory Reset

In case you find the BIG 10 in an undefined operating state (e.g. when no data transfer is possible), press the Reset button on the right side of the casing with a pointed tool (i.e. pen or paper clip) for a short moment (ca. 1 s). The device will then perform a restart and the data connection will be established anew. Contact in any case your service provider before. Pressing the reset button for more than 5 s will cause a factory reset of the device, whereby all performed settings will be lost. A reset to the default configuration should only be realized by experienced users. A Factory Reset may result in complete non-functionality of the BIG 10! Therefore, contact in any case your service provider before!

2.8 Activation / Deactivation of WLAN (only order no. 900220)

Upon initial start-up of the device the WLAN module is deactivated as well. The WLAN module can be activated by keying the WLAN button placed on the right side of the housing below the reset button.
By pressing the WLAN button a second time, the WLAN module will be deactivated again. The current status is indicated through the WLAN status LED.

2.9 Maintenance

Your BIG 10 is maintenance-free. For cleaning please use a dry cloth. Never use aggressive or caustic detergents.



Before cleaning, remove the power supply unit out of the socket, or put the device out of operation.

2.10 Uninstallation of the BIG 10

To uninstall the BIG 10, first disconnect all cables, starting with the power supply unit. After all cables are removed, the device can be taken from the wall.

3 Configuration of the BIG10 router via inbuilt graphical user interface (GUI)

The BIG 10 can easily be configured using its in-built graphical user interface. This can be done using a standard Internet browser (Firefox, Internet Explorer, Safari), which are available at most modern computer today.
To access the Web-GUI proceed as follows:

1. Make sure, that the network settings of your computer allow the automatic IP-address assignment. Please ask you network administrator for further details.
2. Connect your computer with the LAN interface of the BIG 10 using a standard Ethernet cable.
3. After connecting the device, the computer will be assigned by an IP-address automatically.

It is as well possible to use a static IP-address. For this apply your computer the following data:

	Pre-Settings	**User-Settings**
Address Range	192.168.1.2 bis 255	
Subnet Mask	255.255.255.0	
Gateway Address	192.168.1.1	

Open now your Web-Browser and type the following in the address field:
http://192.168.1.1



Note Make sure, that your proxy settings are switched off or set correctly.



The following login window appears after successful connect:

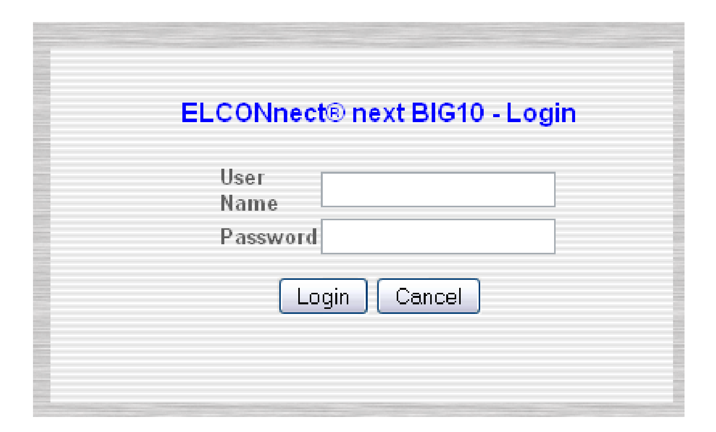


Figure 4: Login window



The login is allowed for the following user:

- The „normal user“ can mainly access status information of the device.
- The „administrative user“ can access all settings of the device.

User		**Pre-Settings**	**User-Settings**
normal user	User name	admin	
	Password	admin	
administrative user	User name	isp-admin	
	Password	isp-admin	

After correct login appears the startup window followed by the system status window after some seconds. This view gives an overview of the network configuration and the actual firmware release.

elcon systemtechnik V0.156 1

2 Home | System Status | (isp-admin) Logout
Setup Wizard | Advanced Setup

System Status

This page provides a quick survey of the network setup and the current connection status of the ELCONnect® next BIG10.

WAN (Internet)	Management (changed)	Data (changed)
IP Address	0.0.0.0	0.0.0.0
Subnet Mask	0.0.0.0	0.0.0.0
Default Gateway	0.0.0.0	0.0.0.0
DNS Server 1	0.0.0.0	0.0.0.0
DNS Server 2	0.0.0.0	0.0.0.0
Connection Type		
VLAN ID	n.a.	n.a.
WAN MAC Address	00:07:23:09:03:40	

LAN (Gateway)	
Network Mode	restricted
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
Firewall	Enabled
LAN MAC Address	00:07:23:09:03:41

Port	Link	Mode	Flow Control	Auto Negotiation	MDI Mode
LAN1	Up	100Mb/s Full Duplex	Disabled	Enabled	MDI
LAN2	Down	?	?	Enabled	?
LAN3	Down	?	?	Enabled	?
LAN4	Down	?	?	Enabled	?
WAN	Down	?	?	Enabled	----

General Information	
Firmware Version	VA_A900217_S800_C049FM_V020.42

Figure 5: System Status

For all further navigation within the user interface are the following red marked areas important:

(1) Change of language; pre-set to German
(2) Basic menus; the following menus are available:
  I. Start page: direct link to the above shown page
  II. System status: direct link to the above shown page
  III. (Current user) Logout: shows the current logged-in user and logs-out from the system; jumps to the login-page
  IV. Configuration assistant: the assistant guides through the most important settings
  V. extended configuration: accessing the manually done, menu guided configuration

The following image shows the most important navigation elements:

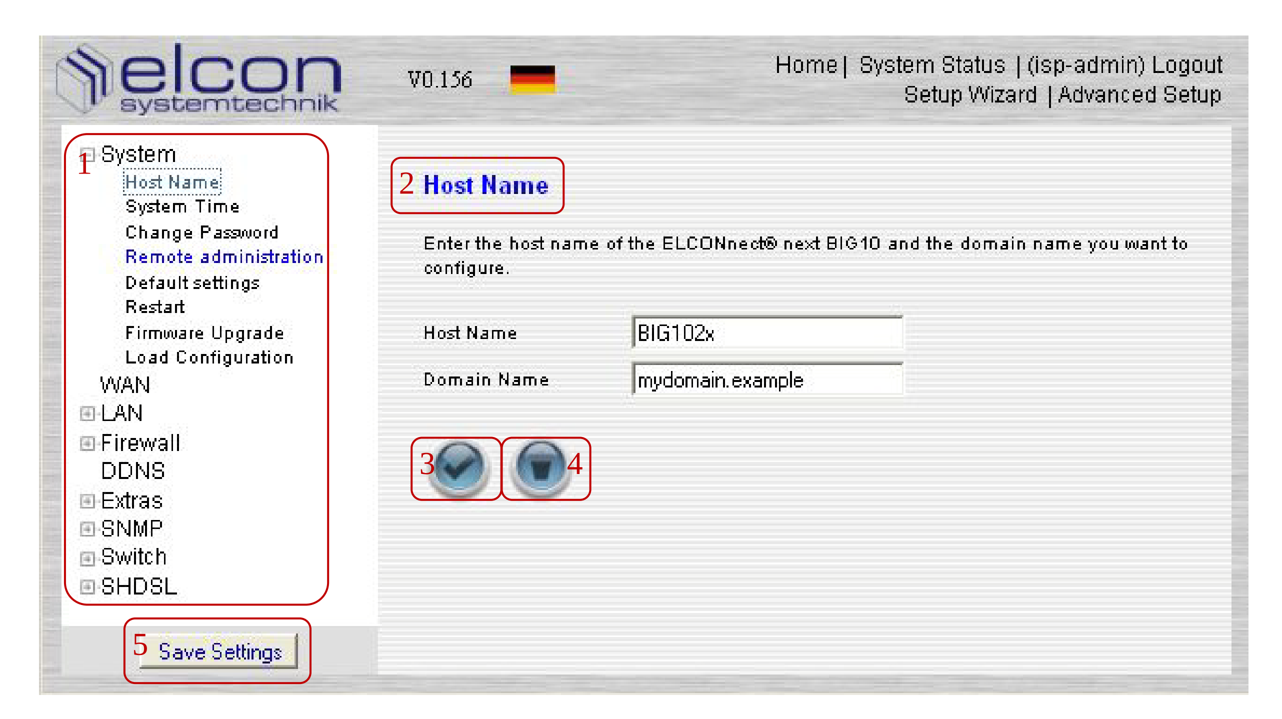


Figure 6: Navigation elements

(1) Menu for manual configuration of the BIG 10
The menu consists of sub-menus, which are visible by clicking on menus. The selected menus and sub-menus are marked blue.
(2) Indication of selected menu or sub-menu
(3) Button for acknowledging the input
(4) Button for deleting / canceling the input
(5) Button for confirm all done settings

Note



It is required to finally press the “Save Settings” button to accept the changes of the configuration. This step is necessarily required because otherwise al settings will be lost after restarting the device.



3.1 System

In this view all system specific settings of the BIG 10 can e processed.

3.1.1 Host Name

Enter the host name of the BIG 10 and the domain name, if required. Both entries are optional.

3.1.2 System Time

The BIG 10 synchronizes its internal time to an Internet time server depending on the chosen time zone. A correct internal time is required to show system log entries with a correct time stamp.

3.1.3 Change password

The access to the user interface is secured by the login name and the appropriate password. In this view, the pre-set password can be changed to your needs as well as the user name.

The time until the user interface logs off for security reasons the user can be set. After expiration the user have to login again.

3.1.4 Remote Administration

If you want to access the user interface remotely, the remote administration must be activated. The access can be limited to an entered IP-address or even IP-address range. The input of an asterisk ("*") means, any IP-address within this range can access the GUI of the device. Entering an asterisk requires that all address fields right to it requires an asterisk too. Accessing the graphical user interface remotely requires entering a port number in addition to the IP-address in the web-browser. The port number can be changed according to your requirements in the range between 1024 – 65535.

Example The input "217.63.*.* " means that all computer with the IP-address between 217.63.0.0 and 217.63.254.254 have access to the device. If the port number is set to 8080, the address should look like: “http://217.63.0.1:8080”.



If it is requested to administrate the BIG 10 from more than one remote location, then can this be configured using a configuration file. Refer to chapter 3.2.

3.1.5 Default settings

If the configuration of the device is in a not working condition is it possible to reset the unit to the factory default (standard settings) values. Two levels of reset are possible:

- „Restore User Parameter“ - resets all from user „admin“ settable values to the default values
- „Restore to factory default settings“ - resets all values to the defaults values.

Click the dedicated button to reset the device to its default values. The restore process requires an additional confirmation.

Warning All own settings are lost after resetting the device to the factory default settings.



3.1.6 Restart

In the rare case the BIG 10 is not responding or is not working properly, the device can be restarted. All settings are preserved, only the device will boot again. Just click at the “Restart” button to release the restart.
This restart can be executed as well pressing the “Reset” button hidden below the side of the housing. Further information can be found at chapter 2.7.

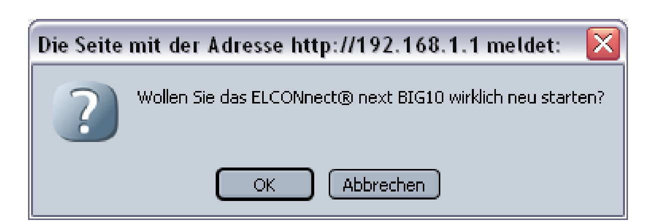


Figure 7: Confirmation prompt upon restart

3.1.7 Firmware upgrade

The device is undergoing a continuous improvement process of functionality and performance. If a new firmware of the device is available then this can be loaded into the unit. Proceed as follows:

1. Store the firmware at your computer.
2. Click „Search/Durchsuchen“, enter the path and file name of the firmware and press the “Apply” button. If it is required to reset the device to its default values after the firmware upgrade, then select the dedicated option checkbox.
3. You will be asked for confirmation of the firmware upgrade.



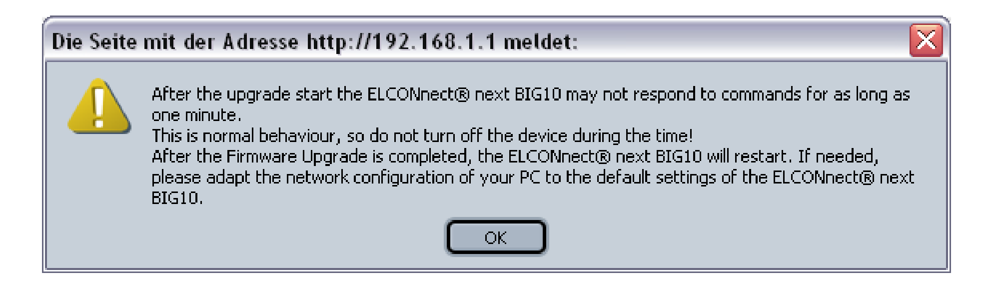


Figure 8: Reference note during Firmware Upgrade

4. Please consider the following messages:

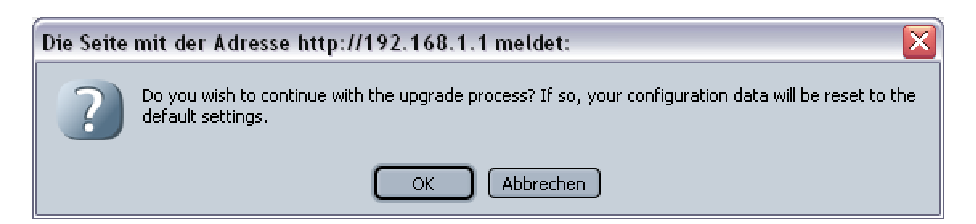


Figure 9: Confirmation prompt during Firmware Upgrade

Note



The firmware upgrade does not change the configuration of your BIG10. All settings are preserved. However, the settings should be saved before!

3.1.8 Import Configuration

The BIG 10 can be configured by use of a configuration file remotely from a central server or locally via the Web-GUI. This speeds up the configuration process of several devices with identical or similar configuration. Refer to next chapter for a central configuration. For a local configuration is a prepared configuration file required, like described in the documentation “Configuration-Documentation.pdf”. This file is a simple text file and can be edited by every standard test editor. Once the file is prepared, then it can be loaded into the device. The configuration can be stored permanently with the “Save Settings” button.

3.2 WAN

The BIG 10 can be configured in different ways. The management access to the device can be secured by means of VLANs. For this it is required to configure the network configuration first. The configuration types can be:

- dynamic configuration („DHCP“), assigning an IP address from a central DHCP server
- static configuration assigning a static IP address
- assigning an IP address via PPPoE

A central located configuration file can be retrieved from a TFTP server in addition by selecting „Opt. 66/67“. So this is a simple way to perform a central device configuration.

Warning If the TFTP server address not accessible or the configuration file cannot be retrieved, then the device is automatically resetting and restarting. This is done in cyclical time frames until a configuration could be retrieved successfully.

The management and data path can be configured after configuring the network parameters. Finally, the DNS server can be assigned either to the management or to the data path.

3.2.1 DHCP Configuration

With the WAN-setting „DHCP“, the device retrieves its IP-address from a DHCP server.

3.2.2 Static Configuration

When using the option „Static“, IP-address,subnet mask, Gateway and DNS-server need to be configured manually. The option „Static“ can be used in case your Internet has made the required data available to you. The setting „Static“allows the assignment of fixed IP-addresses only, whereas DHCP is not supported.

Warning Any changes made on this site have the effect that upon next click upon the button "Save settings" the BIG 10 will automatically perform a restart.

3.2.3 PPPoE

The setting “PPPoE” allows configuring IP address, net mask, gateway and DNS server using a central BRAS server. Chose “PPPoE” if your Internet provider made the username and password available to you. The password must be entered twice in order to avoid wrong entered passwords.
The data for „Service Name“ / „Service Concentrator“ are optional, if provided by the Internet provider.
You can select between connection settings “permanent” or “on demand”. “On demand” requires a “Maximum Idle Time”, the time the connection can stay idle before it will be disconnected.

3.3 LAN

The following menus allow configuring the LAN interface of the BIG 10 and the DHCP server for your local network.

The BIG 10 has a preset IP address for your local network, which can be changed in this menu. By enabling the built-in DHCP-server, the IP-address can be automatically assigned to the devices that are linked to the LAN-ports. The IP-address range and the lease time of the IP address assignment can be changed. The configuration of a domain giving it a domain name is supported.



3.4 Firewall

The BIG 10 provides extensive firewall protection for your network by restricting connection parameters to limit the risk of intrusion and defending against a wide array of common hacker attacks. To ensure remote access to one or several local PCs, despite of the aforesaid, this option has to be configured as specified in chapter NAT. Additional protection is provided by special settings which prevent methods Hackers frequently use for starting an attack. Further, you can set that client computer are fully or partially restricted from Internet access.

3.4.1 Settings

The firewall must be enabled before the BIG 10 can protect your network against hacker attacks from the Internet. In addition, you may also enable specific safety mechanisms: deactivating the options "Enable PING from WAN side" and "Enable PING from LAN side" prevents the BIG 10 responding to Ping packets from the Internet and from the local network respectively. "Drop Port Scan" blocks port scans from the Internet.

3.4.2 IP-Address Filter

The client computer Internet access can be restricted or fully refused, depending on its IP address and according to the port number range chosen. If you wish to enter a certain IP address or port number instead of a defined address range, one and the same number has to be entered twice (e.g. 192.168.1.1 ~ 1). As port number you can enter a number between 1 and 65535.

Note Activating the option IP Address Filter is only possible if the firewall is enabled.



3.4.3 MAC Address Filter

You can block computers, which are linked via LAN, accessing the Internet based on their MAC addresses. Therefore enable the function “MAC Address Filter” and enter the appropriate MAC address of the data terminal.

Note Activating the option MAC Address Filter is only possible if the firewall is enabled.



3.4.4 DDNS

DDNS (Dynamic Domain Name System) allows in case of dynamically assigned WAN IP address that the BIG 10 is always found at the same host name. Different DynDNS providers have been pre-configured. Please contact these providers to receive from them the needed settings.

3.5 WLAN

In this menu can the WLAN access point be configured.

Note  It is required to finally press the “Save Settings” button to accept the changes of the configuration. This step is necessarily required because otherwise all settings will be lost after restarting the device!

3.5.1 Settings

The basic settings of the WLAN access point can in this menu be configured. The access point can be switched on and off with using the checkbox „activate Wireless LAN“. The WLAN SSID can be configured and selected whether this name shall be broadcasted or not.

3.5.2 Safety

The security features of the WLAN access point can be configured in this menu. The encryption standard selected and the WLAN encryption key entered. Furthermore the authentication method local (PSK) or via a central RADIUS server can be configured. .

Note  It is recommended to secure a WLAN network using the latest encryption method! Older methods than WPA2 are not safe anymore.

3.5.3 MAC Address Filter

A MAC address filter can be used to achieve at least a minimum security level of your network. The filter can prevent accessing the device from computer or other network devices with a given MAC address.

Note  MAC addresses can easily be counterfeited. This filter is not a protective instrument against hackers.

3.5.4 Clients

This list shows the MAC addresses of connected WLAN clients.

3.6 Extras

This site allows you to determine upon outgoing (egress) data traffic in how far the DSCP-value (DSCP - DiffServ Code Point) of the IP-packets which are received from the LAN (only network mode router) shall be manipulated by the BIG 10 in the Type-Of-Service-Field of the IP-Header.
If the DSCP-value shall be changed as fixed value, then select "Remarking - active".
Use "Remarking - enhanced", if you wish to have the DSCP-value individually adjusted for certain destination IP-addresses. Up to 20 destinations can be edited.



3.7 SNMP

Simple Network Management Protocol (SNMP) supports the exchange of messages between a network management client and an agent centralizing the management of network elements. The messages consist of “requests” setting (“set”) variables and getting (“get”) variables, which are available at the network elements. It can be used to retrieve statistics, to set configuration parameters and to monitor events within the network. SNMP can communicate via WAN, only. The BIG 10 can create so-called SNMP traps to indicate alarm states. The BIG 10 also has a SNMP agent for the device network management. The central site requires a MIB browser supporting SNMP versions v1/v2/v3.

3.7.1 Basic Setup

Exporting BIG 10 functions to the MIB Browser requires activating and setting SNMP server configurations.

3.7.2 SNMPv3 Setup

The BIG 10 provides security upon SNMP access by means of SNMPv3. You can enable SNMPv3 and configure it in such a way that the users will have authorized access to the SNMP data.

3.8 Switch

The LAN switch of the BIG 10 can be configured in this chapter. The switch functionality is determined by inner and outer ports. The following image shows the port assignment:

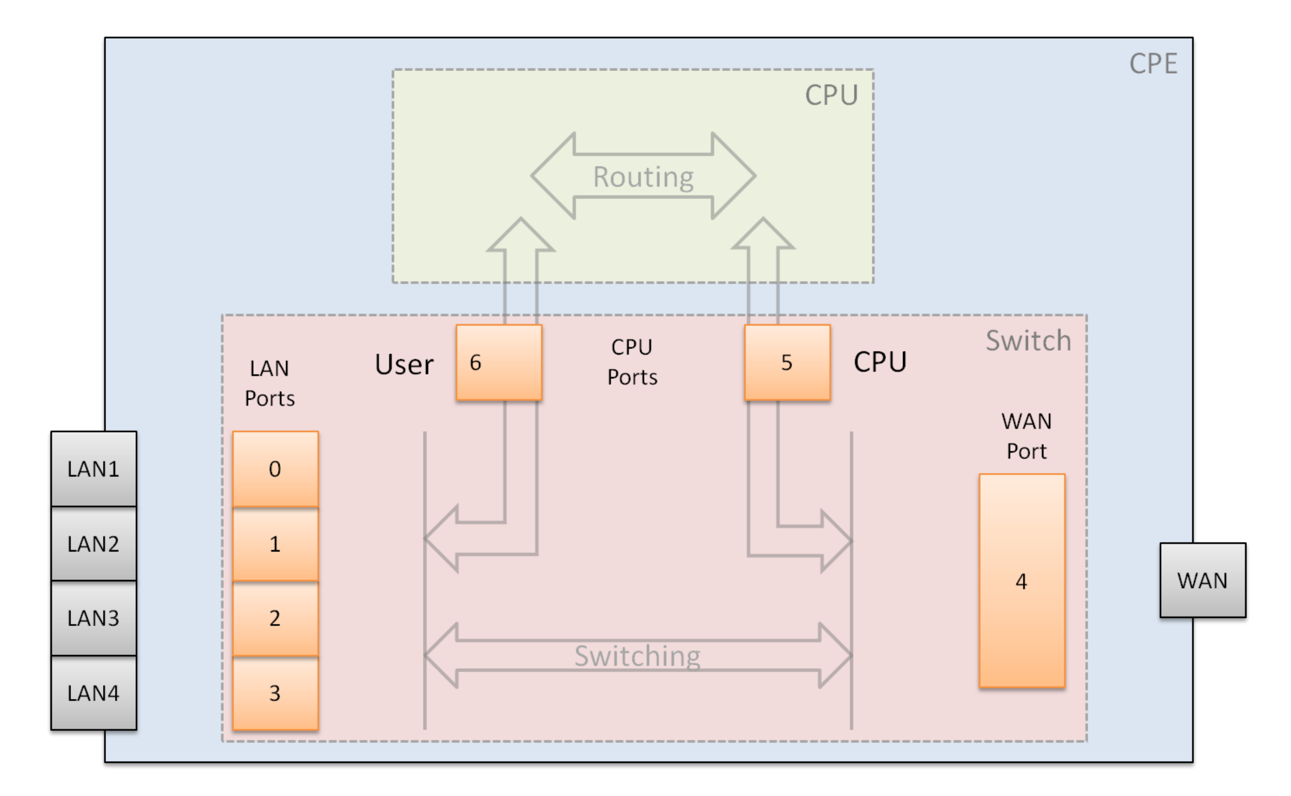


Figure 10: Port assignment

Hereby the system distinguishes between external and internal ports. Outer ports are the LAN ports 0…3, market with LAN1…4 at the device. Port 4 is at the WAN side (DSL) and further used with the term “WAN”. Furthermore two inner ports are available, that are used for routed packets (marked with “User” and “CPU”). The “User” port directs to the LAN side and the “CPU” port to the WAN side. Both ports are connected to the internal CPU.

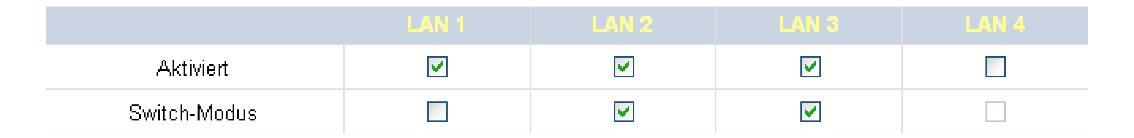
All comprehensive configurations are described in the following chapters. One example helps to understand the options.

3.8.1 Configuration LAN Ports

This chapter allows you to separately configure the LAN-interfaces of the BIG 10.
You have two possibilities to connect LAN ports with the WAN:

1. switched: the LAN ports are directly connected to the WAN port
2. routed: the LAN ports are connected with the WAN port via the CPU (the internal processor).

Example: LAN ports 1…3 are available (LAN4 is deactivated) and LAN2 and LAN3 are directly connected with the WAN interface.



	LAN 1	LAN 2	LAN 3	LAN 4
Aktiviert	☑	☑	☑	☐
Switch-Modus	☐	☑	☑	☐

Figure 11: Example Configuration LAN ports

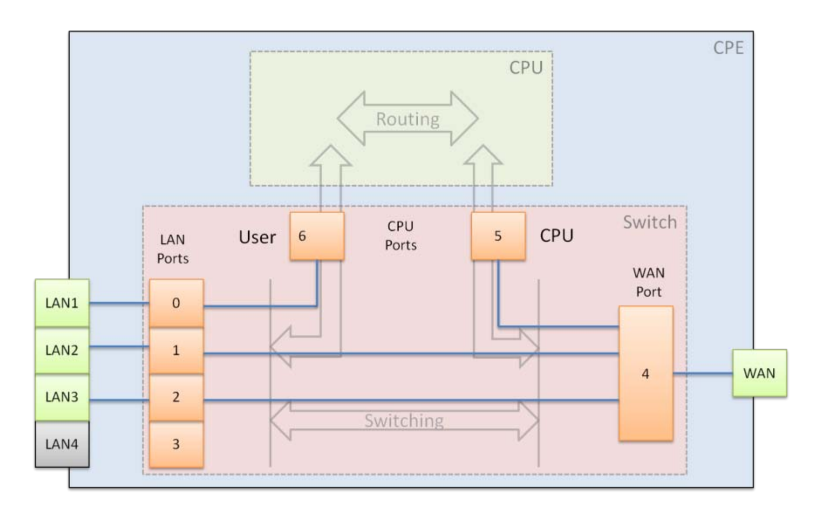


Figure 12: Port assignment as detailed in the sample configuration

Warning Possible Firewall settings are not available for the Ethernet ports set to switch mode. At those ports connected devices are not secured anymore by the internal firewall of the BIG 10!

The LAN port configuration allows setting up the Flow-Control and Auto-Negotiation.



3.8.2 VLAN configuration

This view allows the VLAN configuration of the BIG 10.

Note VLAN configuration requires at minimum one LAN port linked to the WAN (Switch mode, see chapter 3.8.1). The menu „VLAN configuration“ is only visible in this case.



You can configure up to 8 VLAN at the BIG 10. Assign for each VLAN the associated VLAN-ID and VLAN-Priority.

Warning The VLAN-ID 1 is often not supported by many switches. If problems occur, it can be recommended to choose another (2..4094).



Finally select which ports in Switch-Mode VLAN belong to tagged / untagged.

- „-“ means, that the port is no „Member/Mitglied“ of the respective VLAN.
  → only untagged Traffic
- „U“ means, that the port is an „untagged Member/Mitglied“ of the respective VLAN
  → untagged Traffic is marked with VLAN, while Tag is removed for tagged Traffic (VLAN
- „T“ means, that the port is a„Member/Mitglied“ of the respective VLAN
  → only Traffic with the respective VLAN
- „S“ means, that the port adds to any traffic a pre-set VLAN-Tag (Service-Tag)
  → with tagged Traffic the according VLAN-Tag will be removed

3.8.3 QoS Settings

Data can be processed in a specific manner in order to secure services. This is often achieved by “Quality of Service” or simply QoS settings.

QoS improvements can be gained using two ways. First packets can be market via QoS rules to process them prioritized. Secondly can a minimum and maximum bandwidth assigned to ports and queues. Both methods are processed one after the other.

The following picture illustrates the processes of the different QoS methods.

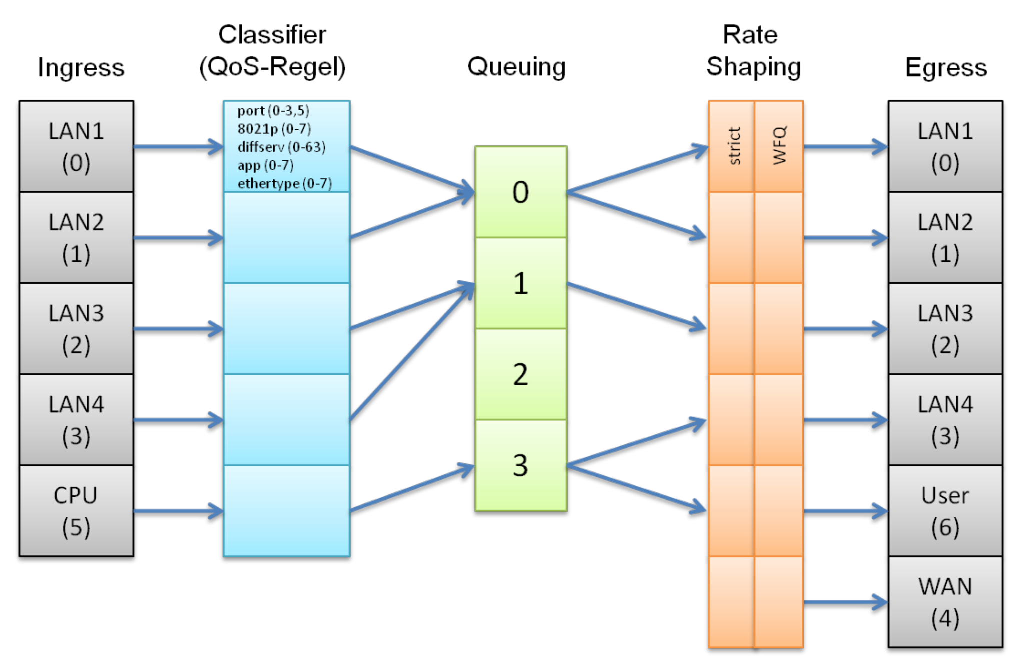


Figure 13: Processing sequence for the miscellaneous QoS-mechanisms

The BIG 10 consists of four internal queues for each port in order to achieve the optimum Quality of Service. Packets are classified into each queue depending on their priority. The unchangeable priorities of the queues are as follows:

Queue	Priority
0	low
1	normal
2	high
3	very high

The QoS rules of all switch ports described next can be assigned to those queues.

3.8.4 QoS Rules

This chapter defines the rules for classification of incoming data traffic. At the same time the data will be classified in one of 4 Priority Queues (highest, high, normal, low).

Note



In order to be able to apply the QoS-rules at the LAN ports, they have to be configured in switch mode. For this, see also chapter 3.8.1.

Rx-Port
This site allows you to determine the way how incoming data traffic is classified at the respective Rx-Port (receiver side of the LAN-/WAN-ports). The data are assigned to one of 4 Priority Queues. To enable this rule, it has to be selected in case of need for the respective Rx-Port in chapter "QoS Settings".

802.1p
This site allows you to determine the way how to classify incoming data traffic by VLAN-priority (IEEE 802.1p). To enable this rule, it is necessary to select it in case of need for the respective LAN port in the chapter "QoS Settings".

DiffServ
This site allows you to determine the way how to classify incoming data traffic by the DSCP (DiffServ Code Point). To enable this rule, it has to be selected in case of need for the respective port in chapter "QoS Settings".

Application
This site allows you to determine the way how to classify incoming data traffic that can be assigned to a certain application. The assignment of the data traffic to an application may be realized by analyzing the source- resp. destination port number in the UDP/TCP packet header. Hereby it is possible to use as criterion the source or the destination port or both at the same time. A port range can be indicated, too. It may range from 1 to 255, beginning with the start port. To enable this rule, it has to be selected in case of need for the respective port in chapter "QoS Settings".

EtherType
This site allows you to determine the way how to classify incoming data traffic by the Ether-Type-Fields in Ethernet-Frame-Header. To enable this rule, it has to be selected in case of need for the respective port in chapter "QoS Settings".

3.8.5 QoS Bandwidth

This site allows you to determine the way how to limit outgoing and incoming data traffic for each port based on priority queues. Proceed with the following steps:

1. Enter the incoming (ingress) bandwidth in kbps.
2. The parameter “WFQ type” defines how the bandwidth settings in kbps (max Mode) or ratio (ratio mode) are done. In “ratio mode” the total bandwidth is distributed over 4 queues depending on the settings. In “max mode” is the bandwidth set to the maximum set value in kbps.
3. Enter the values of the bandwidth distribution for each queue for a guaranteed bandwidth (SPC – strict priority queuing). This is identical to a set bandwidth, if available. and / or
4. Enter the values of the bandwidth distribution for each queue for a weighted bandwidth (WFQ – weighted fair queuing). The assigned bandwidth of WFQ can be up to 3 times the allowable bandwidth for WFQ (example: a total of 40 Mbps are for WFQ available, that is per queue 10 Mbps; means a 30 Mbps can be assigned per queue).

Repeat this for each required port.
The total bandwidth is always equal to the sum of strict (SPC) and weighted (WFQ) bandwidth.

Note The bandwidth can be set in steps of 64 kbps.

Example: The following example shows extensive QoS settings.

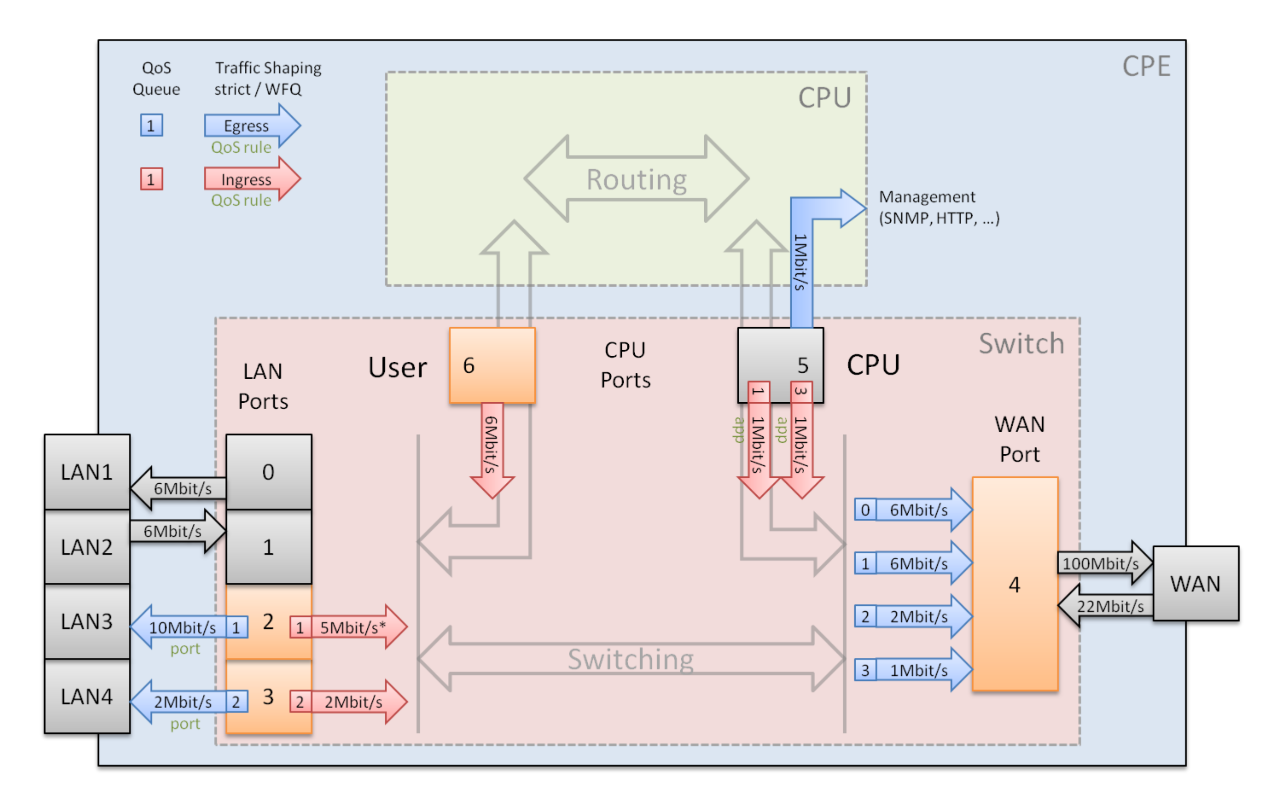


Figure 14: Example: QoS-settings

The device consists of a total bandwidth at the WAN side (SHDSL) of 22 Mbps. The physical LAN ports 1 and 2 are routed via the internal CPU ports (User, CPU). The LAN ports 3 and 4 are directly connected (switched) to the WAN port.

Note



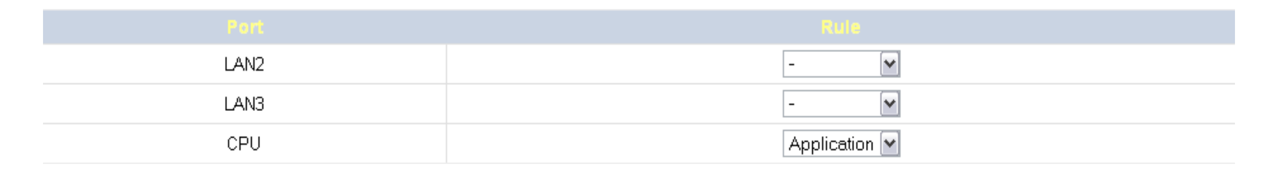
Please consider that all switch ports having a bandwidth of 100 Mbps. Therefor the throughput to the WAN (SHDSL) port is as well 100 Mbps and first limited by the SHDSL bandwidth.

The internal data traffic of the management is a fixed bandwidth of 1 Mbps assigned. The outgoing (egress) traffic is assigned to queue 3 with the highest priority class via the Application QoS rule. In the example http traffic of TCP port 8080 is used.
A special application (e.g. ERP software, VPN etc.) using LAN port 1 or 2 can use a strict bandwidth of 1 Mbps if it’s using the TCP port 30000. The data are assigned to queue 1 (normal priority).
Furthermore the LAN ports 1 and 2 are set to a data rate (up-/downstream) of 6 Mbps for data without any prioritization (like e-mail, Internet data).
LAN port 3 is set to 10 Mbps downstream and 5 Mbps upstream with priority normal (queue 1). An assignment at LAN port 2 is only required, if high UDP data traffic is expected. Otherwise the traffic limitation at the WAN port is sufficient.
LAN port 4 is set to 2 Mbps symmetric with a high priority, therefore queue 2 (e.g. VoIP PBX).



The described example requires the following settings:

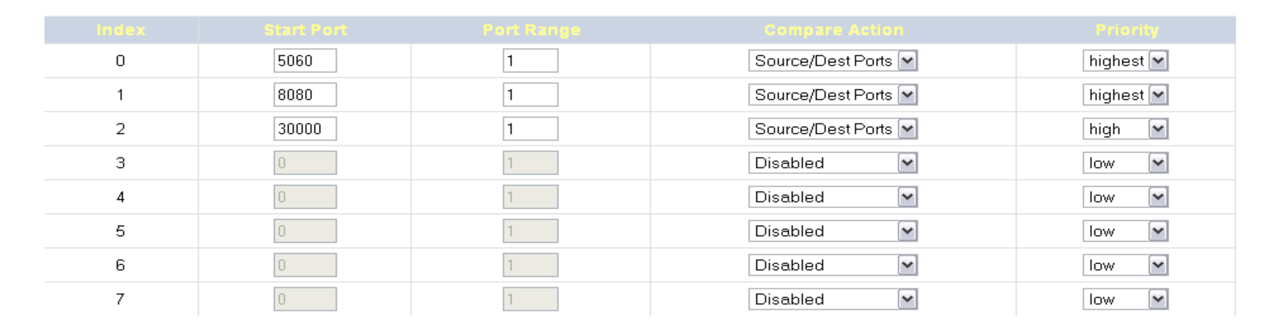
QoS settings:
The internal ports LAN2/3 (physical ports 3/4) are directly switched to the WAN port.



Port	Rule
LAN2	-
LAN3	-
CPU	Application

Figure 15: Example: QoS settings

QoS rules / Application:



Index	Start Port	Port Range	Compare Action	Priority
0	5060	1	Source/Dest Ports	highest
1	8080	1	Source/Dest Ports	highest
2	30000	1	Source/Dest Ports	high
3	0	1	Disabled	low
4	0	1	Disabled	low
5	0	1	Disabled	low
6	0	1	Disabled	low
7	0	1	Disabled	low

Figure 16: Example QoS-rules / Application

QoS bandwidth:



			SPQ (guarantee kbps)				WFQ (Max. kbps)/Ratio			
Port	Ingress [kbps]	WFQ Type	Q3	Q2	Q1	Q0	Q3	Q2	Q1	Q0
LAN2	102400	ratio Mode	102400	102400	102400	102400	102400	102400	102400	102400
LAN3	102400	ratio Mode	102400	102400	102400	102400	102400	102400	102400	102400
WAN	102400	ratio Mode	102400	102400	102400	102400	102400	102400	102400	102400
CPU	102400	ratio Mode	102400	102400	102400	102400	102400	102400	102400	102400
USER	102400	ratio Mode	102400	102400	102400	102400	102400	102400	102400	102400

Figure 17: Example QoS bandwidth

3.8.6 Smart Discard

The BIG 10 supports an innovative function to discard packets earlier depending on its priority. This prevents resource shortages of the QoS queues by packets with lower priority, in case the bandwidth shaping allows only a low bandwidth for a port.
The “Smart Discard” function can be configured for each port separately. The modes have the following function:

Mode	at load	discarded packets
Mode 0	> 0%	0%
Mode 1	> 0% > 75%	0% 25%
Mode 2	> 0% > 50% > 75%	0% 50% 75%
Mode 3	> 0% > 25% > 50%	0% 25% 50%

3.8.7 Port Security

Port security allows filtering Ethernet frames at a certain LAN port coming from dynamically learned or statically edited MAC addresses.

Note: The Port Security function is disabled at the relevant ports, in case the MAC-address filter is inactive and value "0" has been selected for MAC-address limitation.



3.8.8 Statistics

On this page you can get statistical information for each switch port of your BIG 10.

3.8.9 Monitoring

This site allows you to configure, in how far incoming and/or outgoing data traffic of a discretionary LAN Port or resp. WAN Port shall be mirrored to another LAN Port.

3.9 SHDSL

The following pages show the SHDSL configuration and states of the BIG 10.

3.9.1 Config

On this page specific SHDSL parameter can be configured.



Operating Mode
The operating mode offers multiple setting options and can be configured in RT (“remote terminal” or CPE) or COT (“central office terminal”) mode.

EFM G.hs Mode
ITU G.hs according to ITU-T G.994.1 and IEEE802.3ah

PMMS Mode (Line Probing)
Line Probing according to ITU-T G.991.2 (2004)

PMMS Target Margin
Desired Signal Noise Ratio for the PMMS-mode

3.9.2 Status

Line states of all lines are shown. The view can be refreshed manually („Refresh” button) or automatically pushing the “Auto Refresh” button.

Line state

Down (Idle) / Down (Ready)	Link down
PCS Sync	Bonding Group established
G.hs Line Probing	Negotiation of line parameters
G.hs Transfer	Negotiation of line parameters
Data Mode	Line is in Data Mode

Data rate
The following data rates (in kbps) depending on the configuration of the COT side can be achieved with the BIG 10:

Annex	**Modulation**	**1-pair resp. 2-wire**	**2-pair resp. 4-wire**	**3-pair resp. 6-wire**	**4-pair resp. 8-wire**
Annex A/B	TC-PAM-16	192… 2304	384… 4608	576… 6912	768… 9216
Annex AF/BG	TC-PAM-16	192… 3840	384… 7680	576…11520	768…15360
	TC-PAM-32	768… 5696	1536…11392	2304…17088	3072…22784

Loop Attenuation (dB)
Measured loop attenuation in dB; longer loop length results in high loop attenuation.

SNR (dB)
The SNR (“signal noise ratio”) is an index of the line quality. The larger the SNR the better is the line quality. The SNR ranges from -10 dB to 21 dB.

3.9.3 Performance

This view shows actual performance values of all lines.

Time Stamp
Shows the time after activation of the NT function or the elapsed time (24h format) after activation of the SHDSL line.

TMP (total measurement period)
Full duration (time interval) of counting performance data; will be reset after 15 minutes = 900 seconds

ES (errored seconds)
number of seconds with errors

SES (severe errored seconds)
number of seconds with major alarms

CRC6 (cyclic redundancy check)
number of CRC6 errors

LOSW (los of sync word)
number of LOSW errors

UAS (unavailable seconds)
number of seconds without data transmission

3.9.4 Performance History

For line selection please click at line number above the table. The performance history shows all errors which occurred in the 15-minute intervals over one day (24 hours).



4 Technical data

WAN interface (SHDSL)

Norm	ITU-T G.991.2 G.SHDSL.bis; SHDSL 2/4 line pairs
Bandwidth	high symmetrical bandwidth (up to 22 Mbps) thanks to EFM-Bonding support (IEEE 802.3-2004) and ATM-Bonding (support of M-Pair mode)
Connector	1 × RJ45

ATM

- ATM layer acc. to I.361
- AAL5 acc. to I.363.5
- VPI/VCI range configurable
- support of OAM F4/F5, AIS, RDI, and loopback

LAN interface (Ethernet)

Norm	standard Ethernet protocol IEEE 802.3, IEEE 802.1q, 802.1d, native Multicast,
VLAN	VLAN double tagging as per IEEE 803.2ac VLAN support for management and user data DSCP remarking
Ethernet features	10/100 Base-T, MDI/MDIX-Autosensing, TCP/IP
Bridge functions	transparent layer 2 bridging
max. frame size	1536 bytes (switch mode) 1518 bytes (router mode, restricted mode)
Connector	4 × RJ45

Router functions

- TCP/IP v4
- NAT
  - virtual Server
  - Port Mapping
  - virtual DMZ
- DHCP-Client/Server
- PPPoE
- static IP
- Firewall
- DynDNS

Quality of Service

- Strict Priority (SPQ) & Weighted Fair Queuing (WFQ)
- definition of service classes
  - Port-based
  - 802-1p
  - DSCP
  - Application based (TCP port)
  - Ethertype
- bandwidth management (shaping), Bandwidth limitation (limiting)

OAM

- Dying Gasp support
- NTP
- MAC Address Filter
- statistical data or history

WLAN interface (only order no. 900220)

Access Point	acc. to IEEE802.11b/g
802.11g Data rate	54, 48, 36, 24, 12, 9, 9 Mbps
802.11b Data rate	11, 5.5, 2, 1 Mbps
Safety	64- / 128-bit WEB; WPA-PSK, WPA2-PSK, WPA, WPA2
Transmit power	up to 100 mW
Antenna	external

Management and configuration

Configuration	via integrated Web-GUI (local); SNMP v2 / v3; DHCP / TFTP (remote via configuration file)
Security	password for configuration

Power supply of plug-in power supply module

Operating voltage range	100 V … 240 V ∼
Frequency range	50 Hz … 60 Hz
Current consumption	≤ 0.5 A
Connector	Euro plug

Power supply of BIG 10

Nominal voltage	12 V ⎓
Current consumption	< 1.2 A

Casing

Design version	Plastic casing with integrated display elements and physical interfaces
Display elements	4 (5) LEDs for status information
Dimensions	240.4 mm × 160.4 mm × 48.2 mm (W × D × H)
Colour	signal white (RAL 9003), jet black (RAL 9005)
Weight	1.0 kg

Environmental conditions (according to ETS 300 019)

Storage and transport	Temperature: -40°C ... +70°C Humidity: 0% ... 85% (not condensing)
Operation	Temperature: 0°C ... +45°C Humidity: 10% ... 85% (not condensing)

Standards, Certificates

EMC	ETSI EN 300 386, EN 55022 Class B, ETSI ES 201 468, ITU-T K.21
Safety	EN 60950-1



5 Important notes

5.1 Manufacturer´s declaration

The manufacturer confirms that the ELCONnect next BIG 10 Router has been designed for the transfer of data information and, subject to its proper usage, complies with the relevant safety standards and the applicable EMC requirements

5.2 Warranty

This documentation compiled by ELCON Systemtechnik GmbH is based on best available technology. However, although applying due diligence, it is impossible to exclude all mistakes and technical inaccuracies. In view of the rapid technological progress, ELCON reserves the right to modifications and improvements without prior notification. For this reason ELCON assumes no liability for the content of this document.

Further, ELCON shall not be responsible for any loss or incorrect use of information or data which may result from using this document. In addition, ELCON cannot be held liable for damages, whether direct or indirect (including, but not limited to, financial losses, delayed business transactions, disruption of business or similar consequences), incurred as a result of improper use of the equipment.

This documentation has been made to explain the functionality of the BIG 10 Router. It describes installation and application of the device and its supplementary equipment, drivers and software tools (if required). Detailed information, addressing client-specific solutions, can be taken from the relevant user manual.

Further information on the operation of peripheral equipment and installations, in particular about the installation of cable TV networks, computer hardware and the available access technologies, can be received from your telecommunications network operator or Internet Service Provider, or the respective user manuals.
Note: This documentation may describe performance features which cannot be used in the specific application case.

5.3 Rights and trademarks

With respect to the information contained in this documentation ELCON provides no warranties as for the non-existence of industrial property rights (trademarks, patents, utility models, etc.). Generally used trademarks, trade names, company and product names are subject to the respective trademark, patent, utility model or registered design rights.

The information in this document must not be copied, neither in full nor in extracts, translated, reprinted or transferred in any other way.

The purchase of software and equipment shall be governed by the General Terms and Conditions for the Sale and Supply of Products and Services and the License Conditions of ELCON Systemtechnik GmbH.



Declaration of Conformity

We ELCON Systemtechnik GmbH

(Manufacturer or his Authorised Representative established within the EAA)

Obere Hauptstraße. 10
09232 Hartmannsdorf

(Address)

declare under our sole responsibility that the product

ELCONnect® next BIG102X Router
(PCB identification number 102631-3X)

(Name, type or model)

to which this declaration relates is in conformity with the following standard(s) or other normative document(s)

EN 60950-1:2006
EN 300 386 V1.4.1 (2008-04)
EN 55022:2006
EN 61000-3-2:2006
EN 61000-3-3:2006

(Title and/or number and date of issue of the standard(s) or other normative document(s) if applicable)

following the provisions of directive

2004/108/EC	EMC-Directive
2006/95/EC	Low Voltage Directive
1999/5/EC	R&TTE-Directive
No 278/2009	Commission Regulation for implementing Directive 2005/32/EC

(Number and title of the European Council Directives which applies)

Registration number of Type Examination Certificate: 10/08

Year in which the CE marking was affixed: 2010

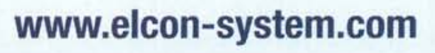
Hartmannsdorf, 2010-06-18

(Place and date of issue)

Werner Neubauer
Managing Director

(Name and signature or equivalent marking of authorized person)







Declaration of Conformity

We ELCON Systemtechnik GmbH

(Manufacturer or his Authorised Representative established within the EAA)

Obere Hauptstraße. 10
09232 Hartmannsdorf

(Address)

declare under our sole responsibility that the product

ELCONnect® next BIG104X WLAN Router
(PCB identification number 102631-3X)

(Name, type or model)

to which this declaration relates is in conformity with the following standard(s) or other normative document(s)

EN 60950-1:2006
EN 300 386 V1.4.1 (2008-04)
EN 55022:2006
ETSI EN 300 328 (2006-10)
ETSI EN 301 489-1 (2008-04)
EN 61000-3-2:2006
EN 61000-3-3:2006

(Title and/or number and date of issue of the standard(s) or other normative document(s) if applicable)

following the provisions of directive

2004/108/EC	EMC-Directive
2006/95/EC	Low Voltage Directive
1999/5/EC	R&TTE-Directive
No 278/2009	Commission Regulation for implementing Directive 2005/32/EC

(Number and title of the European Council Directives which applies)

Registration number of Type Examination Certificate: 10/03

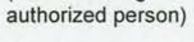
Year in which the CE marking was affixed: 2010

Hartmannsdorf, 2010-10-27

(Place and date of issue)

Markus Königshofer
Managing Director

(Name and signature or equivalent marking of authorized person)





www.elcon-system.com



Typenschild
(nur Art.-Nr. 900220)

Aufkleber MAC-Adresse
(nur Art.-Nr. 900220)